PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-187101

(43)Date of publication of application : 04.07.2003

(51)Int.Cl. G06F 17/60
H04L 9/32
H04N 7/167
H04N 7/173

(21)Application number : 2001-385453

(22)Date of filing : 19.12.2001

(71)Applicant : SONY CORP

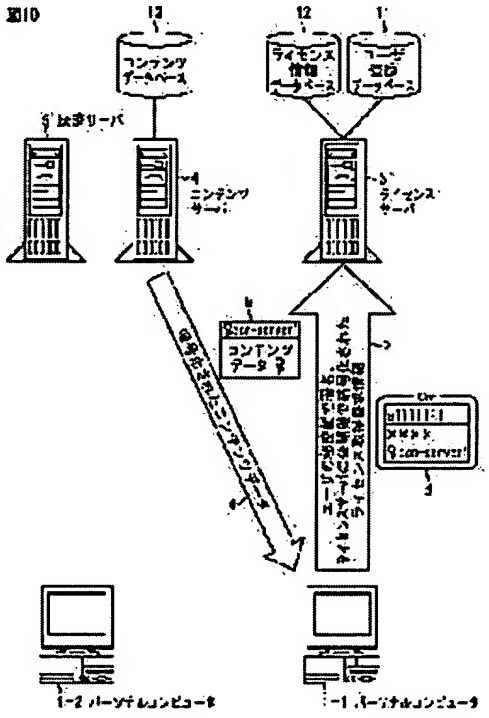
(72)Inventor : CHIN KOGUN

(54) INFORMATION PROCESSOR, INFORMATION PROCESSING METHOD, STORAGE MEDIUM, INFORMATION PROCESSING SYSTEM AND PROGRAM

(57)Abstract:

PROBLEM TO BE SOLVED: To protect a copyright of a content when making content transferable by peer-to-peer.

SOLUTION: Transmission and receipt of encrypted content data between a content server 4 and a personal computer 1-1 is executed without using public key cryptosystem as shown by (a) in a Figure. User information containing information ID showing the source of the content data is described in a field attached to the content data as shown by b in the Figure. Since the user information is encrypted by the public key of a license server 3, only the license server 3 can read it. Electronically signed preview license acquisition request information or general license acquisition request information is transmitted to the license server 3 as shown by c in the Figure. The information showing the source of the content data is described in the license acquisition request information as shown by d in the Figure.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2003－187101
（Ｐ２００３－１８７１０１Ａ）
(43)公開日　平成15年７月４日(2003.7.4)

(51)Int.Cl.[7]	識別記号	Ｆ Ｉ		テーマコード（参考）
G06F 17/60	312	G06F 17/60	312	5C064
	142		142	5J104
	302		302	E
	512		512	
	ZEC		ZEC	

審査請求　未請求　請求項の数26　ＯＬ　（全29頁）　最終頁に続く

(21)出願番号　特願2001－385453（Ｐ2001－385453）
(22)出願日　平成13年12月19日(2001.12.19)

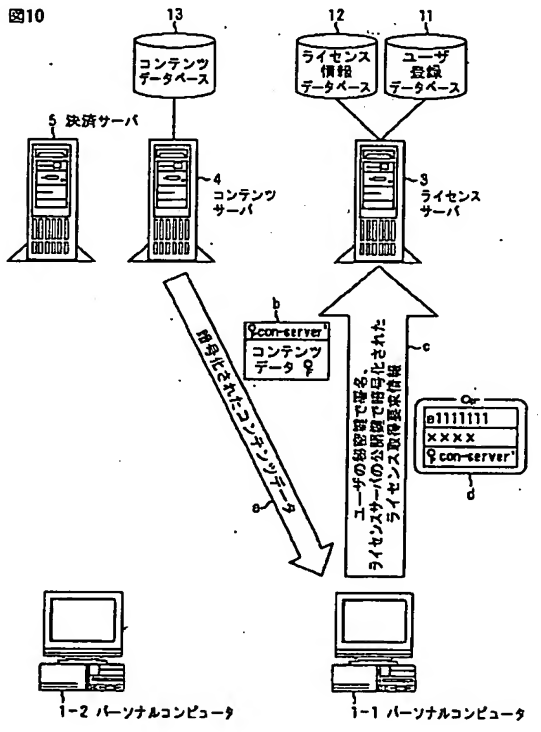
(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号
(72)発明者　陳　向群
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(74)代理人　100082131
弁理士　稲本　義雄

Ｆターム(参考)　5C064 BA07 BB02 BB07 BC01 BC17
BC18 BC22 BC23 BD02 BD08
BD09 CA14 CB01 CC01 CC04
5J104 AA09 LA03 LA06 MA05

(54)【発明の名称】情報処理装置および情報処理方法、記録媒体、情報処理システム、並びに、プログラム

(57)【要約】
【課題】　コンテンツをピアツーピアで授受可能とした場合にその著作権を守る。
【解決手段】　図中ａに示されるように、コンテンツサーバ４とパーソナルコンピュータ１－１との暗号化されたコンテンツデータの送受信は、公開鍵暗号方式を用いずに実行される。図中ｂに示されるように、コンテンツデータに添付しているフィールドには、このコンテンツデータの配信元を示す情報（ＩＤ）を含むユーザ情報が記載されている。ユーザ情報は、ライセンスサーバ３の公開鍵で暗号化されているため、ライセンスサーバ３しか読み取ることが出来ない。暗号化され、電子署名されたプレビューライセンス取得要求情報、もしくは通常ラインセンス取得要求情報は、図中ｃに示されるように、ライセンスサーバ３に送信される。ラインセンス取得要求情報には、図中ｄに示されるように、コンテンツデータの配信元を示す情報が記載されている。

図10



1

【特許請求の範囲】

【請求項１】　コンテンツを取得する取得手段と、
前記コンテンツに添付されている第１の情報、前記コンテンツを特定するための第２の情報、および自分自身を特定することができる第３の情報を含む第４の情報を生成する生成手段と、
前記生成手段により生成された前記第４の情報を送信する第１の送信手段と、
前記コンテンツを再生するために必要な第５の情報を受信する受信手段と、
前記受信手段により受信された前記第５の情報に添付されている第６の情報を抽出する抽出手段と、
前記抽出手段により抽出された前記第６の情報を、前記コンテンツに添付されている前記第１の情報に代わって、前記コンテンツに添付させる情報添付手段とを備えることを特徴とする情報処理装置。

【請求項２】　前記情報添付手段により前記第６の情報が添付された前記コンテンツを、他の情報処理装置に送信する第２の送信手段を更に備えることを特徴とする請求項１に記載の情報処理装置。

【請求項３】　前記第１の情報、および前記第６の情報は、前記第４の情報の送信先の公開鍵で暗号化されていることを特徴とする請求項１に記載の情報処理装置。

【請求項４】　前記第５の情報は、前記コンテンツを条件付で再生させるための第１のライセンス情報と、前記コンテンツを完全に再生させるための第２のライセンス情報のいずれかであることを特徴とする請求項１に記載の情報処理装置。

【請求項５】　前記生成手段により生成された前記第４の情報を、暗号化する暗号化手段を更に備えることを特徴とする請求項１に記載の情報処理装置。

【請求項６】　前記暗号化手段は、前記第４の情報を、前記第４の情報の送信先の公開鍵で暗号化し、自分自身の秘密鍵で電子署名を施すことを特徴とする請求項５に記載の情報処理装置。

【請求項７】　前記受信手段により受信された前記第５の情報を復号する復号手段を更に備えることを特徴とする請求項１に記載の情報処理装置。

【請求項８】　コンテンツの取得を制御する取得制御ステップと、
前記コンテンツに添付されている第１の情報、前記コンテンツを特定するための第２の情報、および自分自身を特定することができる第３の情報を含む第４の情報を生成する生成ステップと、
前記生成ステップの処理により生成された前記第４の情報の送信を制御する送信制御ステップと、
前記コンテンツを再生するために必要な第５の情報の受信を制御する受信制御ステップと、
前記受信制御ステップの処理により受信が制御された前記第５の情報に添付されている第６の情報を抽出する抽出ステップと、
前記抽出ステップの処理により抽出された前記第６の情報を、前記コンテンツに添付されている前記第１の情報に代わって、前記コンテンツに添付させる情報添付ステップとを含むことを特徴とする情報処理方法。

【請求項９】　コンテンツの取得を制御する取得制御ステップと、
前記コンテンツに添付されている第１の情報、前記コンテンツを特定するための第２の情報、および自分自身を特定することができる第３の情報を含む第４の情報を生成する生成ステップと、
前記生成ステップの処理により生成された前記第４の情報の送信を制御する送信制御ステップと、
前記コンテンツを再生するために必要な第５の情報の受信を制御する受信制御ステップと、
前記受信制御ステップの処理により受信が制御された前記第５の情報に添付されている第６の情報を抽出する抽出ステップと、
前記抽出ステップの処理により抽出された前記第６の情報を、前記コンテンツに添付されている前記第１の情報に代わって、前記コンテンツに添付させる情報添付ステップとを含むことを特徴とするコンピュータが読み取り可能なプログラムが記録されている記録媒体。

【請求項１０】　コンテンツの取得を制御する取得制御ステップと、
前記コンテンツに添付されている第１の情報、前記コンテンツを特定するための第２の情報、および自分自身を特定することができる第３の情報を含む第４の情報を生成する生成ステップと、
前記生成ステップの処理により生成された前記第４の情報の送信を制御する送信制御ステップと、
前記コンテンツを再生するために必要な第５の情報の受信を制御する受信制御ステップと、
前記受信制御ステップの処理により受信が制御された前記第５の情報に添付されている第６の情報を抽出する抽出ステップと、
前記抽出ステップの処理により抽出された前記第６の情報を、前記コンテンツに添付されている前記第１の情報に代わって、前記コンテンツに添付させる情報添付ステップとを含む処理をコンピュータに実行させることを特徴とするプログラム。

【請求項１１】　コンテンツを取得する取得手段と、
前記コンテンツに添付されている第１の情報、前記コンテンツを特定するための第２の情報、および自分自身を特定することができる第３の情報を含む第４の情報を生成する生成手段と、
前記生成手段により生成された前記第４の情報を送信する送信手段と、
前記コンテンツを再生するために必要な第５の情報を受信する受信手段と、

2

自分自身を特定することができる第６の情報を、前記第４の情報の送信先の公開鍵で暗号化する暗号化手段と、前記暗号化手段により暗号化された前記第６の情報を、前記コンテンツに添付されている前記第１の情報に代わって、前記コンテンツに添付させる情報添付手段とを備えることを特徴とする情報処理装置。

【請求項１２】　コンテンツの取得を制御する取得制御ステップと、
前記コンテンツに添付されている第１の情報、前記コンテンツを特定するための第２の情報、および自分自身を特定することができる第３の情報を含む第４の情報を生成する生成ステップと、
前記生成ステップの処理により生成された前記第４の情報の送信を制御する送信制御ステップと、
前記コンテンツを再生するために必要な第５の情報の受信を制御する受信制御ステップと、
自分自身を特定することができる第６の情報を、前記第４の情報の送信先の公開鍵で暗号化する暗号化ステップと、
前記暗号化ステップの処理により暗号化された前記第６の情報を、前記コンテンツに添付されている前記第１の情報に代わって、前記コンテンツに添付させる情報添付ステップとを含むことを特徴とする情報処理方法。

【請求項１３】　コンテンツの取得を制御する取得制御ステップと、
前記コンテンツに添付されている第１の情報、前記コンテンツを特定するための第２の情報、および自分自身を特定することができる第３の情報を含む第４の情報を生成する生成ステップと、
前記生成ステップの処理により生成された前記第４の情報の送信を制御する送信制御ステップと、
前記コンテンツを再生するために必要な第５の情報の受信を制御する受信制御ステップと、
自分自身を特定することができる第６の情報を、前記第４の情報の送信先の公開鍵で暗号化する暗号化ステップと、
前記暗号化ステップの処理により暗号化された前記第６の情報を、前記コンテンツに添付されている前記第１の情報に代わって、前記コンテンツに添付させる情報添付ステップとを含むことを特徴とするコンピュータが読み取り可能なプログラムが記録されている記録媒体。

【請求項１４】　コンテンツの取得を制御する取得制御ステップと、
前記コンテンツに添付されている第１の情報、前記コンテンツを特定するための第２の情報、および自分自身を特定することができる第３の情報を含む第４の情報を生成する生成ステップと、
前記生成ステップの処理により生成された前記第４の情報の送信を制御する送信制御ステップと、
前記コンテンツを再生するために必要な第５の情報の受信を制御する受信制御ステップと、
自分自身を特定することができる第６の情報を、前記第４の情報の送信先の公開鍵で暗号化する暗号化ステップと、
前記暗号化ステップの処理により暗号化された前記第６の情報を、前記コンテンツに添付されている前記第１の情報に代わって、前記コンテンツに添付させる情報添付ステップとを含む処理をコンピュータに実行させることを特徴とするプログラム。

【請求項１５】　コンテンツを再生させるために用いられる、前記コンテンツに固有の第１の情報を記録する第１の記録手段と、
前記コンテンツを保有する他の情報処理装置から、前記コンテンツに添付されている第２の情報、前記コンテンツを特定するための第３の情報、および、前記他の情報処理装置を特定するための第４の情報を含む第５の情報を受信する受信手段と、
前記第１の記録手段に記録されている前記第１の情報のうち、前記第３の情報によって特定される前記コンテンツに対応する前記第１の情報を抽出する抽出手段と、
前記他の情報処理装置を特定する情報を少なくとも含む第６の情報を生成する第１の生成手段と、
前記第１の生成手段により生成された前記第６の情報、および前記抽出手段により抽出された前記第１の情報を少なくとも含む第７の情報を生成する第２の生成手段と、
前記第２の生成手段により生成された前記第７の情報を前記第４の情報により特定される前記他の情報処理装置へ送信する送信手段とを備えることを特徴とする情報処理装置。

【請求項１６】　前記第１の生成手段により生成された前記第６の情報を、自分自身の公開鍵で暗号化する暗号化手段を更に備え、
前記第２の生成手段は、前記暗号化手段により暗号化された前記第６の情報、および前記抽出手段により抽出された前記第１の情報を少なくとも含む第７の情報を生成することを特徴とする請求項１５に記載の情報処理装置。

【請求項１７】　前記受信手段により受信された前記第５の情報に含まれている前記第２の情報を自分自身の秘密鍵を用いて復号する復号手段を更に備え、
前記第２の情報は、前記公開鍵により暗号化されている情報であることを特徴とする請求項１５に記載の情報処理装置。

【請求項１８】　前記第１の情報は、前記コンテンツを条件付で再生させるための第１のライセンス情報と、前記コンテンツを完全に再生させるための第２のライセンス情報のいずれかであることを特徴とする請求項１５に記載の情報処理装置。

【請求項１９】　前記第２の生成手段により生成された

前記第７の情報を暗号化する暗号化手段を更に備えることを特徴とする請求項１５に記載の情報処理装置。

【請求項２０】　前記暗号化手段は、前記第７の情報を、前記第４の情報により特定される前記他の情報処理装置の公開鍵で暗号化し、自分自身の秘密鍵で電子署名を施すことを特徴とする請求項１９に記載の情報処理装置。

【請求項２１】　前記受信手段により受信された前記第５の情報を復号する復号手段を更に備えることを特徴とする請求項１５に記載の情報処理装置。

【請求項２２】　前記受信手段により受信された前記第５の情報に含まれている、前記第２の情報、前記第３の情報、および前記第４の情報を記録する第２の記録手段と、

前記第２の記録手段により記録された前記第２の情報、前記第３の情報、および前記第４の情報を基に、前記コンテンツに関する情報を解析する解析手段とを更に備えることを特徴とする請求項１５に記載の情報処理装置。

【請求項２３】　コンテンツを再生させるために用いられる、前記コンテンツに固有の第１の情報の記録を制御する記録制御ステップと、

前記コンテンツを保有する他の情報処理装置からの、前記コンテンツに添付されている第２の情報、前記コンテンツを特定するための第３の情報、および、前記他の情報処理装置を特定するための第４の情報を含む第５の情報の受信を制御する受信制御ステップと、

前記記録制御ステップの処理により記録が制御されている前記第１の情報のうち、前記第３の情報によって特定される前記コンテンツに対応する前記第１の情報を抽出する抽出ステップと、

前記他の情報処理装置を特定する情報を少なくとも含む第６の情報を生成する第１の生成ステップと、

前記第１の生成ステップの処理により生成された前記第６の情報、および前記抽出ステップの処理により抽出された前記第１の情報を少なくとも含む第７の情報を生成する第２の生成ステップと、

前記第２の生成ステップの処理により生成された前記第７の情報の、前記第４の情報により特定される前記他の情報処理装置への送信を制御する送信制御ステップとを含むことを特徴とする情報処理方法。

【請求項２４】　コンテンツを再生させるために用いられる、前記コンテンツに固有の第１の情報の記録を制御する記録制御ステップと、

前記コンテンツを保有する他の情報処理装置からの、前記コンテンツに添付されている第２の情報、前記コンテンツを特定するための第３の情報、および、前記他の情報処理装置を特定するための第４の情報を含む第５の情報の受信を制御する受信制御ステップと、

前記記録制御ステップの処理により記録が制御されている前記第１の情報のうち、前記第３の情報によって特定

される前記コンテンツに対応する前記第１の情報を抽出する抽出ステップと、

前記他の情報処理装置を特定する情報を少なくとも含む第６の情報を生成する第１の生成ステップと、

前記第１の生成ステップの処理により生成された前記第６の情報、および前記抽出ステップの処理により抽出された前記第１の情報を少なくとも含む第７の情報を生成する第２の生成ステップと、

前記第２の生成ステップの処理により生成された前記第７の情報の、前記第４の情報により特定される前記他の情報処理装置への送信を制御する送信制御ステップとを含むことを特徴とするコンピュータが読み取り可能なプログラムが記録されている記録媒体。

【請求項２５】　コンテンツを再生させるために用いられる、前記コンテンツに固有の第１の情報の記録を制御する記録制御ステップと、

前記コンテンツを保有する他の情報処理装置からの、前記コンテンツに添付されている第２の情報、前記コンテンツを特定するための第３の情報、および、前記他の情報処理装置を特定するための第４の情報を含む第５の情報の受信を制御する受信制御ステップと、

前記記録制御ステップの処理により記録が制御されている前記第１の情報のうち、前記第３の情報によって特定される前記コンテンツに対応する前記第１の情報を抽出する抽出ステップと、

前記他の情報処理装置を特定する情報を少なくとも含む第６の情報を生成する第１の生成ステップと、

前記第１の生成ステップの処理により生成された前記第６の情報、および前記抽出ステップの処理により抽出された前記第１の情報を少なくとも含む第７の情報を生成する第２の生成ステップと、

前記第２の生成ステップの処理により生成された前記第７の情報の、前記第４の情報により特定される前記他の情報処理装置への送信を制御する送信制御ステップとを含む処理をコンピュータに実行させることを特徴とするプログラム。

【請求項２６】　コンテンツを取得して再生する、少なくとも一つの第１の情報処理装置と、

前記コンテンツを再生させるための情報を前記第１の情報処理装置に送信する第２の情報処理装置とによって構成される情報処理システムにおいて、

前記第１の情報処理装置は、

前記コンテンツを取得する取得手段と、

前記コンテンツに添付されている第１の情報、前記コンテンツを特定するための第２の情報、および自分自身を特定することができる第３の情報を含む第４の情報を生成する第１の生成手段と、

前記第１の生成手段により生成された前記第４の情報を前記第２の情報処理装置へ送信する第１の送信手段と、

前記第２の情報処理装置から送信された前記コンテンツ

を再生するために必要な第５の情報を受信する第１の受信手段と、
前記受信手段により受信された前記第５の情報に添付されている第６の情報を抽出する第１の抽出手段と、
前記第１の抽出手段により抽出された前記第６の情報を、前記コンテンツに添付されている前記第１の情報に代わって、前記コンテンツに添付させる情報添付手段とを備え、
前記第２の情報処理装置は、
前記コンテンツを再生させるために用いられる、前記コンテンツに固有の第７の情報を記録する記録手段と、
前記第１の情報処理装置から、前記第１の情報、前記第２の情報、および、
前記第３の情報を含む前記第４の情報を受信する第２の受信手段と、
前記記録手段に記録されている前記第７の情報のうち、前記第２の情報によって特定される前記コンテンツに対応する前記第７の情報を抽出する第２の抽出手段と、
前記第１の情報処理装置を特定する情報を少なくとも含む前記第６の情報を生成する第２の生成手段と、
前記第２の生成手段により生成された前記第６の情報、および前記第２の抽出手段により抽出された前記第７の情報を少なくとも含む前記第５の情報を生成する第３の生成手段と、
前記第３の生成手段により生成された前記第５の情報を前記第３の情報により特定される前記第１の情報処理装置へ送信する第２の送信手段とを備えることを特徴とする情報処理システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、情報処理装置および情報処理方法、記録媒体、情報処理システム、並びに、プログラムに関し、特に、サービスを受けるユーザ同士でコンテンツをピアツーピアで授受することが可能なコンテンツ配信サービスを提供する場合に用いて好適な情報処理装置および情報処理方法、記録媒体、情報処理システム、並びに、プログラムに関する。

【０００２】

【従来の技術】パーソナルコンピュータの記憶容量の増加、および音声や映像の再生技術の向上にともなって、パーソナルコンピュータ内部に楽曲データや映像データなどを記録し、再生して楽しむユーザが増えている。

【０００３】楽曲データや映像データなど、いわゆるコンテンツデータは、インターネットなどを介して、コンテンツ配信サービスを行っている事業者が運営するウェブサイトからダウンロードすることができる。また、パーソナルコンピュータ間で、コンテンツをピアツーピアで授受することも可能である。

【０００４】

【発明が解決しようとする課題】しかしながら、ユーザが保有するパーソナルコンピュータ間で、コンテンツをピアツーピアで授受する場合、コンテンツの著作権を守るのが非常に困難である。そのため、許可されたユーザ（例えば、料金を支払ったユーザ）に、復号鍵とともに、暗号化されたコンテンツデータを配信することが考えられている。

【０００５】しかしながら、コンテンツデータを暗号化して、ピアツーピアでコンテンツデータを受け取ったユーザが、コンテンツデータを視聴することが出来ないようにしてしまっては、ピアツーピアを利用してコンテンツを広く流通させることが出来なくなる。

【０００６】更に、ユーザは、料金を支払う前に、そのコンテンツデータは自分の嗜好にあったものか否かを確かめるために、例えば、音楽データであれば試聴するなどして、コンテンツデータの内容を確認したいと考える。そのため、コンテンツ配信サービス事業者は、暗号化されたコンテンツデータとは別に、例えば、復号鍵を用いることなく視聴することができる試聴用データ（例えば、コンテンツデータの一部など）を配信する必要が生じている。

【０００７】本発明はこのような状況に鑑みてなされたものであり、コンテンツデータの購入前にユーザにコンテンツの試聴を可能とし、コンテンツの著作権を守りつつ、ピアツーピアを利用して、コンテンツを広く流通させることができるようにし、更に、コンテンツの流れをトレーシングすることができるようにするものである。

【０００８】

【課題を解決するための手段】本発明の第１の情報処理装置は、コンテンツを取得する取得手段と、コンテンツに添付されている第１の情報、コンテンツを特定するための第２の情報、および自分自身を特定することができる第３の情報を含む第４の情報を生成する生成手段と、生成手段により生成された第４の情報を送信する第１の送信手段と、コンテンツを再生するために必要な第５の情報を受信する受信手段と、受信手段により受信された第５の情報に添付されている第６の情報を抽出する抽出手段と、抽出手段により抽出された第６の情報を、コンテンツに添付されている第１の情報に代わって、コンテンツに添付させる情報添付手段とを備えることを特徴とする。

【０００９】情報添付手段により第６の情報が添付されたコンテンツを、他の情報処理装置に送信する第２の送信手段を更に備えるようにすることができる。

【００１０】第１の情報、および第６の情報は、第４の情報の送信先の公開鍵で暗号化されているものとすることができる。

【００１１】第５の情報は、コンテンツを条件付で再生させるための第１のライセンス情報と、コンテンツを完全に再生させるための第２のライセンス情報のいずれかであるものとすることができる。

【００１２】生成手段により生成された第４の情報を、暗号化する暗号化手段を更に備えるようにすることができる。

【００１３】暗号化手段には、第４の情報を、第４の情報の送信先の公開鍵で暗号化させ、自分自身の秘密鍵で電子署名を施させるようにすることができる。

【００１４】受信手段により受信された第５の情報を復号する復号手段を更に備えさせるようにすることができる。

【００１５】本発明の第１の情報処理方法は、コンテンツの取得を制御する取得制御ステップと、コンテンツに添付されている第１の情報、コンテンツを特定するための第２の情報、および自分自身を特定することができる第３の情報を含む第４の情報を生成する生成ステップと、生成ステップの処理により生成された第４の情報の送信を制御する送信制御ステップと、コンテンツを再生するために必要な第５の情報の受信を制御する受信制御ステップと、受信制御ステップの処理により受信が制御された第５の情報に添付されている第６の情報を抽出する抽出ステップと、抽出ステップの処理により抽出された第６の情報を、コンテンツに添付されている第１の情報に代わって、コンテンツに添付させる情報添付ステップとを含むことを特徴とする。

【００１６】本発明の第１の記録媒体に記録されているプログラムは、コンテンツの取得を制御する取得制御ステップと、コンテンツに添付されている第１の情報、コンテンツを特定するための第２の情報、および自分自身を特定することができる第３の情報を含む第４の情報を生成する生成ステップと、生成ステップの処理により生成された第４の情報の送信を制御する送信制御ステップと、コンテンツを再生するために必要な第５の情報の受信を制御する受信制御ステップと、受信制御ステップの処理により受信が制御された第５の情報に添付されている第６の情報を抽出する抽出ステップと、抽出ステップの処理により抽出された第６の情報を、コンテンツに添付されている第１の情報に代わって、コンテンツに添付させる情報添付ステップとを含むことを特徴とする。

【００１７】本発明の第１のプログラムは、コンテンツの取得を制御する取得制御ステップと、コンテンツに添付されている第１の情報、コンテンツを特定するための第２の情報、および自分自身を特定することができる第３の情報を含む第４の情報を生成する生成ステップと、生成ステップの処理により生成された第４の情報の送信を制御する送信制御ステップと、コンテンツを再生するために必要な第５の情報の受信を制御する受信制御ステップと、受信制御ステップの処理により受信が制御された第５の情報に添付されている第６の情報を抽出する抽出ステップと、抽出ステップの処理により抽出された第６の情報を、コンテンツに添付されている第１の情報に代わって、コンテンツに添付させる情報添付ステップとを含む処理をコンピュータに実行させることを特徴とする。

【００１８】本発明の第２の情報処理装置は、コンテンツを取得する取得手段と、コンテンツに添付されている第１の情報、コンテンツを特定するための第２の情報、および自分自身を特定することができる第３の情報を含む第４の情報を生成する生成手段と、生成手段により生成された第４の情報を送信する送信手段と、コンテンツを再生するために必要な第５の情報を受信する受信手段と、自分自身を特定することができる第６の情報を、第４の情報の送信先の公開鍵で暗号化する暗号化手段と、暗号化手段により暗号化された第６の情報を、コンテンツに添付されている第１の情報に代わって、コンテンツに添付させる情報添付手段とを備えることを特徴とする。

【００１９】本発明の第２の情報処理方法は、コンテンツの取得を制御する取得制御ステップと、コンテンツに添付されている第１の情報、コンテンツを特定するための第２の情報、および自分自身を特定することができる第３の情報を含む第４の情報を生成する生成ステップと、生成ステップの処理により生成された第４の情報の送信を制御する送信制御ステップと、コンテンツを再生するために必要な第５の情報の受信を制御する受信制御ステップと、自分自身を特定することができる第６の情報を、第４の情報の送信先の公開鍵で暗号化する暗号化ステップと、暗号化ステップの処理により暗号化された第６の情報を、コンテンツに添付されている第１の情報に代わって、コンテンツに添付させる情報添付ステップとを含むことを特徴とする。

【００２０】本発明の第２の記録媒体に記録されているプログラムは、コンテンツの取得を制御する取得制御ステップと、コンテンツに添付されている第１の情報、コンテンツを特定するための第２の情報、および自分自身を特定することができる第３の情報を含む第４の情報を生成する生成ステップと、生成ステップの処理により生成された第４の情報の送信を制御する送信制御ステップと、コンテンツを再生するために必要な第５の情報の受信を制御する受信制御ステップと、自分自身を特定することができる第６の情報を、第４の情報の送信先の公開鍵で暗号化する暗号化ステップと、暗号化ステップの処理により暗号化された第６の情報を、コンテンツに添付されている第１の情報に代わって、コンテンツに添付させる情報添付ステップとを含むことを特徴とする。

【００２１】本発明の第２のプログラムは、コンテンツの取得を制御する取得制御ステップと、コンテンツに添付されている第１の情報、コンテンツを特定するための第２の情報、および自分自身を特定することができる第３の情報を含む第４の情報を生成する生成ステップと、生成ステップの処理により生成された第４の情報の送信を制御する送信制御ステップと、コンテンツを再生する

ために必要な第５の情報の受信を制御する受信制御ステップと、自分自身を特定することができる第６の情報を、第４の情報の送信先の公開鍵で暗号化する暗号化ステップと、暗号化ステップの処理により暗号化された第６の情報を、コンテンツに添付されている第１の情報に代わって、コンテンツに添付させる情報添付ステップとを含む処理をコンピュータに実行させることを特徴とする。

【００２２】本発明の第３の情報処理装置は、コンテンツを再生させるために用いられる、コンテンツに固有の第１の情報を記録する第１の記録手段と、コンテンツを保有する他の情報処理装置から、コンテンツに添付されている第２の情報、コンテンツを特定するための第３の情報、および、他の情報処理装置を特定するための第４の情報を含む第５の情報を受信する受信手段と、第１の記録手段に記録されている第１の情報のうち、第３の情報によって特定されるコンテンツに対応する第１の情報を抽出する抽出手段と、他の情報処理装置を特定する情報を少なくとも含む第６の情報を生成する第１の生成手段と、第１の生成手段により生成された第６の情報、および抽出手段により抽出された第１の情報を少なくとも含む第７の情報を生成する第２の生成手段と、第２の生成手段により生成された第７の情報を第４の情報により特定される他の情報処理装置へ送信する送信手段とを備えることを特徴とする。

【００２３】第１の生成手段により生成された第６の情報を、自分自身の公開鍵で暗号化する暗号化手段を更に備えるようにすることができ、第２の生成手段には、暗号化手段により暗号化された第６の情報、および抽出手段により抽出された第１の情報を少なくとも含む第７の情報を生成させるようにすることができる。

【００２４】受信手段により受信された第５の情報に含まれている第２の情報を自分自身の秘密鍵を用いて復号する復号手段を更に備えさせるようにすることができ、第２の情報は、公開鍵により暗号化されている情報であるものとすることができる。

【００２５】第１の情報は、コンテンツを条件付で再生させるための第１のライセンス情報と、コンテンツを完全に再生させるための第２のライセンス情報のいずれかであるものとすることができる。

【００２６】第２の生成手段により生成された第７の情報を暗号化する暗号化手段を更に備えさせるようにすることができる。

【００２７】暗号化手段には、第７の情報を、第４の情報により特定される他の情報処理装置の公開鍵で暗号化させ、自分自身の秘密鍵で電子署名を施させるようにすることができる。

【００２８】受信手段により受信された第５の情報を復号する復号手段を更に備えさせるようにすることができる。

【００２９】受信手段により受信された第５の情報に含まれている、第２の情報、第３の情報、および第４の情報を記録する第２の記録手段と、第２の記録手段により記録された第２の情報、第３の情報、および第４の情報を基に、コンテンツに関する情報を解析する解析手段を更に備えさせるようにすることができる。

【００３０】本発明の第３の情報処理方法は、コンテンツを再生させるために用いられる、コンテンツに固有の第１の情報の記録を制御する記録制御ステップと、コンテンツを保有する他の情報処理装置からの、コンテンツに添付されている第２の情報、コンテンツを特定するための第３の情報、および、他の情報処理装置を特定するための第４の情報を含む第５の情報の受信を制御する受信制御ステップと、記録制御ステップの処理により記録が制御されている第１の情報のうち、第３の情報によって特定されるコンテンツに対応する第１の情報を抽出する抽出ステップと、他の情報処理装置を特定する情報を少なくとも含む第６の情報を生成する第１の生成ステップと、第１の生成ステップの処理により生成された第６の情報、および抽出ステップの処理により抽出された第１の情報を少なくとも含む第７の情報を生成する第２の生成ステップと、第２の生成ステップの処理により生成された第７の情報の、第４の情報により特定される他の情報処理装置への送信を制御する送信制御ステップとを含むことを特徴とする。

【００３１】本発明の第３の記録媒体に記録されているプログラムは、コンテンツを再生させるために用いられる、コンテンツに固有の第１の情報の記録を制御する記録制御ステップと、コンテンツを保有する他の情報処理装置からの、コンテンツに添付されている第２の情報、コンテンツを特定するための第３の情報、および、他の情報処理装置を特定するための第４の情報を含む第５の情報の受信を制御する受信制御ステップと、記録制御ステップの処理により記録が制御されている第１の情報のうち、第３の情報によって特定されるコンテンツに対応する第１の情報を抽出する抽出ステップと、他の情報処理装置を特定する情報を少なくとも含む第６の情報を生成する第１の生成ステップと、第１の生成ステップの処理により生成された第６の情報、および抽出ステップの処理により抽出された第１の情報を少なくとも含む第７の情報を生成する第２の生成ステップと、第２の生成ステップの処理により生成された第７の情報の、第４の情報により特定される他の情報処理装置への送信を制御する送信制御ステップとを含むことを特徴とする。

【００３２】本発明の第３のプログラムは、コンテンツを再生させるために用いられる、コンテンツに固有の第１の情報の記録を制御する記録制御ステップと、コンテンツを保有する他の情報処理装置からの、コンテンツに添付されている第２の情報、コンテンツを特定するための第３の情報、および、他の情報処理装置を特定するた

めの第４の情報を含む第５の情報の受信を制御する受信制御ステップと、記録制御ステップの処理により記録が制御されている第１の情報のうち、第３の情報によって特定されるコンテンツに対応する第１の情報を抽出する抽出ステップと、他の情報処理装置を特定する情報を少なくとも含む第６の情報を生成する第１の生成ステップと、第１の生成ステップの処理により生成された第６の情報、および抽出ステップの処理により抽出された第１の情報を少なくとも含む第７の情報を生成する第２の生成ステップと、第２の生成ステップの処理により生成された第７の情報の、第４の情報により特定される他の情報処理装置への送信を制御する送信制御ステップとを含む処理をコンピュータに実行させることを特徴とする。

【００３３】本発明の情報処理システムは、第１の情報処理装置が、コンテンツを取得する取得手段と、コンテンツに添付されている第１の情報、コンテンツを特定するための第２の情報、および自分自身を特定することができる第３の情報を含む第４の情報を生成する第１の生成手段と、第１の生成手段により生成された第４の情報を第２の情報処理装置へ送信する第１の送信手段と、第２の情報処理装置から送信されたコンテンツを再生するために必要な第５の情報を受信する第１の受信手段と、受信手段により受信された第５の情報に添付されている第６の情報を抽出する第１の抽出手段と、第１の抽出手段により抽出された第６の情報を、コンテンツに添付されている第１の情報に代わって、コンテンツに添付させる情報添付手段とを備え、第２の情報処理装置が、コンテンツを再生させるために用いられる、コンテンツに固有の第７の情報を記録する記録手段と、第１の情報処理装置から、第１の情報、第２の情報、および、第３の情報を含む第４の情報を受信する第２の受信手段と、記録手段に記録されている第７の情報のうち、第２の情報によって特定されるコンテンツに対応する第７の情報を抽出する第２の抽出手段と、第１の情報処理装置を特定する情報を少なくとも含む第６の情報を生成する第２の生成手段と、第２の生成手段により生成された第６の情報、および第２の抽出手段により抽出された第７の情報を少なくとも含む第５の情報を生成する第３の生成手段と、第３の生成手段により生成された第５の情報を第３の情報により特定される第１の情報処理装置へ送信する第２の送信手段とを備えることを特徴とする。

【００３４】本発明の第１の情報処理装置および情報処理方法、並びにプログラムにおいては、コンテンツが取得され、コンテンツに添付されている第１の情報、コンテンツを特定するための第２の情報、および自分自身を特定することができる第３の情報を含む第４の情報が生成され、生成された第４の情報が送信され、コンテンツを再生するために必要な第５の情報が受信され、第５の情報に添付されている第６の情報が抽出され、抽出された第６の情報が、コンテンツに添付されている第１の情報に代わって、コンテンツに添付される。

【００３５】本発明の第２の情報処理装置および情報処理方法、並びにプログラムにおいては、コンテンツが取得され、コンテンツに添付されている第１の情報、コンテンツを特定するための第２の情報、および自分自身を特定することができる第３の情報を含む第４の情報が生成され、生成された第４の情報が送信され、コンテンツを再生するために必要な第５の情報が受信され、自分自身を特定することができる第６の情報が、第４の情報の送信先の公開鍵で暗号化され、暗号化された第６の情報が、コンテンツに添付されている第１の情報に代わって、コンテンツに添付される。

【００３６】本発明の第３の情報処理装置および情報処理方法、並びにプログラムにおいては、コンテンツを再生させるために用いられる、コンテンツに固有の第１の情報が記録され、コンテンツを保有する他の情報処理装置から、コンテンツに添付されている第２の情報、コンテンツを特定するための第３の情報、および、他の情報処理装置を特定するための第４の情報を含む第５の情報が受信され、記録されている第１の情報のうち、第３の情報によって特定されるコンテンツに対応する第１の情報が抽出され、他の情報処理装置を特定する情報を少なくとも含む第６の情報が生成され、生成された第６の情報、抽出された第１の情報を少なくとも含む第７の情報が生成され、生成された第７の情報が、第４の情報により特定される他の情報処理装置へ送信される。

【００３７】本発明の情報処理システムにおいては、第１の情報処理装置で、コンテンツが取得され、コンテンツに添付されている第１の情報、コンテンツを特定するための第２の情報、および自分自身を特定することができる第３の情報を含む第４の情報が生成され、生成された第４の情報が第２の情報処理装置へ送信され、第２の情報処理装置から送信されたコンテンツを再生するために必要な第５の情報が受信され、第５の情報に添付されている第６の情報が抽出され、抽出された第６の情報が、コンテンツに添付されている第１の情報に代わって、コンテンツに添付され、第２の情報処理装置で、コンテンツを再生させるために用いられる、コンテンツに固有の第７の情報が記録され、第１の情報処理装置から、第１の情報、第２の情報、および、第３の情報を含む第４の情報が受信され、記録されている第７の情報のうち、第２の情報によって特定されるコンテンツに対応する第７の情報が抽出され、第１の情報処理装置を特定する情報を少なくとも含む第６の情報が生成され、生成された第６の情報、および抽出された第７の情報を少なくとも含む第５の情報が生成され、生成された第５の情報が第３の情報により特定される第１の情報処理装置へ送信される。

【００３８】

【発明の実施の形態】以下、図を参照して、本発明の実

施の形態について説明する。

【００３９】図１は、本発明を適応したコンテンツ配信サービスを提供するために利用されるネットワーク構成図である。

【００４０】ユーザが保有するパーソナルコンピュータ１－１乃至１－ｎは、インターネット２を介して、ライセンスサーバ３、コンテンツサーバ４、および決済サーバ５と接続されている。

【００４１】パーソナルコンピュータ１－１乃至１－ｎは、インターネット２を介して、コンテンツサーバ４から、コンテンツを受信（ダウンロード）する。コンテンツデータには、例えば、楽曲データ、画像データ、静止画像データ、動画像データ、あるいは、動画像データと音声データとによる映像データなど、様々な形態のものがある。

【００４２】コンテンツサーバ４は、パーソナルコンピュータ１－１乃至１－ｎを利用するユーザが所望するコンテンツデータを、コンテンツデータベース１３から検索して、インターネット２を介して、パーソナルコンピュータ１－１乃至１－ｎに送信する。コンテンツデータベース１３に記録されているコンテンツデータは、暗号化されている。コンテンツサーバ４は、例えば、インターネット２上に、コンテンツのダウンロードを行うことができるウェブサイト（ダウンロードサイト）を公開するようにしても良い。

【００４３】図２を用いて、コンテンツデータベース１３にコンテンツデータとともに登録されているコンテンツ管理テーブルについて説明する。

【００４４】コンテンツ管理テーブルには、コンテンツを表す固有のＩＤであるコンテンツＩＤ、コンテンツを記録している場所を示すアドレス情報、および対応するコンテンツを再生する場合に利用されるライセンスＩＤなどが記録されている。ライセンスＩＤは、通常ライセンス用のライセンスＩＤと、プレビューライセンス用のライセンスＩＤが登録されている。コンテンツサーバ４はライセンスを発行せず、コンテンツデータベース１３も、コンテンツに対するライセンスを保存しているわけではないので、コンテンツ管理テーブルでは、ライセンスＩＤを必ずしも登録する必要はない。しかしながら、ライセンスに含まれるコンテンツを復号するための復号鍵（ライセンスキー）は、コンテンツサーバ４が、それぞれのコンテンツを暗号化した暗号化鍵と一対を成す鍵であるので、コンテンツ管理テーブルにおいて、ライセンスＩＤとコンテンツＩＤとの関係が管理されているほうが望ましい。

【００４５】ここで、通常ライセンスとは、コンテンツを完全に再生することが出来るライセンスであり、プレビューライセンスとは、その内容の一部を確認するための、いわゆるお試し再生（例えば、コンテンツの一部の再生など）ができるライセンスである。

【００４６】また、パーソナルコンピュータ１－１乃至パーソナルコンピュータ１－ｎは、コンテンツサーバ４から受信したコンテンツデータを、自分自身以外のパーソナルコンピュータ１－１乃至パーソナルコンピュータ１－ｎと、ピアツーピアで送受信することが可能である。更に、他のパーソナルコンピュータから受信したコンテンツデータを、他のパーソナルコンピュータにピアツーピアで同様にして送信することができるのは言うまでもない。

【００４７】このようにして流通されるコンテンツデータは、暗号化されており、コンテンツデータを受信するだけでは、再生して、視聴することができない。そこで、パーソナルコンピュータ１－１乃至１－ｎは、インターネット２を介して、ライセンスサーバ３に、コンテンツデータを再生するためのライセンスの送信を要求する。

【００４８】パーソナルコンピュータ１－１乃至１－ｎがライセンスサーバ３からライセンスを受信するためには、予め、後述する処理によりユーザ登録を実行する必要がある。ライセンスサーバ３は、パーソナルコンピュータ１－１乃至１－ｎよりユーザ登録情報の入力を受け、登録されるユーザのそれぞれに固有の番号であるユーザＩＤを発行する。

【００４９】ライセンスサーバ３には、ユーザ登録データベース１１およびライセンス情報データベース１２が接続されており、ユーザが、パーソナルコンピュータ１－１乃至１－ｎを用いてコンテンツサーバ４から配信される、あるいは、ピアツーピアで、他のパーソナルコンピュータからコピーしたコンテンツを再生するためのライセンスを発行する。

【００５０】ライセンスには、コンテンツデータの全てを復号することが可能な通常ライセンスと、ユーザがコンテンツの内容を確認するための制限的な再生、すなわち、コンテンツの一部のみ、あるいは、ビットレートや解像度が落とされた（いわゆる、デグレードされた）コンテンツを再生することができるプレビューライセンスがある。パーソナルコンピュータ１－１乃至１－ｎは、通常ライセンス、もしくはプレビューライセンスをライセンスサーバに要求する。

【００５１】ライセンスには、通常ライセンスであるかプレビューライセンスであるかを示すライセンスステータス、所定のコンテンツを復号するための復号鍵（ライセンスキー）、必要に応じて、コピーガード情報、コンテンツを再生する場合の制限（例えば、再生可能期間や再生可能回数、あるいは、コピー可能回数など）を示す制限情報、および、コンテンツの流通経路をトレーシングするために用いられるユーザ情報が含まれている。ユーザ情報には、コンテンツの配信元を示すために、例えば、ユーザＩＤなど、ユーザを特定することができる情報が少なくとも含まれており、ライセンスサーバ３の公

開鍵で暗号化されている。また、ライセンスには、上述する以外にも、コンテンツに付随する各種情報などを含ませるようにしてもよい。

【００５２】決済サーバ５は、通常ライセンス発行に先立って、パーソナルコンピュータ１－１乃至１－ｎを保有するユーザと、ライセンスサーバ３の管理者との課金処理を実行するものである。課金方法としては、例えば、クレジットカード決済、プリペイドカードを用いた決済、電子マネーによる決済など、いずれの方法を用いるようにしても良い。

【００５３】また、コンテンツサーバ４から配信され、パーソナルコンピュータ１－１乃至１－ｎ間をピアツーピアで授受されるコンテンツデータには、ユーザ情報を記載するためのフィールドが付加されている。

【００５４】例えば、コンテンツサーバ４から、コンテンツが配信された場合、そのフィールドには、コンテンツサーバ４から配信されたことを示す情報を含む、コンテンツサーバ４のユーザ情報が記載されている。そして、ユーザＡが保有するパーソナルコンピュータ１－１で、対応するコンテンツのライセンスが取得された場合（プレビューでも、通常でもよい）、ライセンスには、ユーザＡを特定するための情報を含むユーザ情報が含まれており、そのフィールドに記載されている情報は、ユーザＡのユーザ情報に書き換えられる。

【００５５】そして、そのコンテンツが、ユーザＡが保有するパーソナルコンピュータ１－１からユーザＢが保有するパーソナルコンピュータ１－２へピアツーピアで送信される場合、そのフィールドには、コンテンツの配信元となるユーザＡのユーザのユーザ情報が記載されている。そして、ユーザＢが保有するパーソナルコンピュータ１－２において、ライセンスが取得された場合、ライセンスには、ユーザＢのユーザ情報が含まれており、コンテンツに添付されているフィールドに記載されている情報は、ユーザＢのユーザ情報に書き換えられる。

【００５６】本システムにおいては、ライセンスサーバ３と登録済みのパーソナルコンピュータ１－１乃至１－ｎとが、インターネット２を介して、安全性の高い情報の授受を行うために、公開鍵暗号方式を利用するものとする。従って、ライセンスサーバ３は、ユーザ登録時に、登録されるユーザの公開鍵を入手するとともに、ライセンスサーバの公開鍵を登録されたユーザが利用しているパーソナルコンピュータ１－１乃至１－ｎに送信する。

【００５７】公開鍵暗号方式とは、データ暗号化方式の１つである。公開鍵暗号方式では、データ送信者のデータの暗号化と、データ受信者のデータの復号とで、それぞれ異なる鍵（ビット列）が使用される（公開鍵暗号方式に対して、秘密鍵暗号方式では、暗号化と復号の双方で同じ鍵を用いる）。

【００５８】公開鍵暗号方式においては、「公開鍵」と「秘密鍵」という２種類の鍵が利用される。このうち秘密鍵は、それを生成したユーザが安全な場所に保管しておき、他人にはいっさい公開しない。一方の公開鍵は、データの送信元となる可能性がある（自分に対してデータを送る可能性がある）相手に広く配布しておく。具体的には、電子メールに添付して相手に送付してもよいし、公開鍵を管理するサービスを行う事業者に預けて、誰でも参照できるようにしてもよい。そしてデータの送信者は、受信先が発行した公開鍵を入手し、受信先の公開鍵で、送信するデータを暗号化する。こうして暗号化されたデータを復号するには、暗号化に使われた公開鍵に対応する秘密鍵が必要である。このため秘密鍵を持たない第三者がデータを傍受したとしても、データを復号することはできない。

【００５９】「公開鍵」と「秘密鍵」の鍵ペアを生成するためには、いくつかの方法があるが、Rivest、Shamir、およびAdlemanによって提唱されたＲＳＡアルゴリズムが有名である。ＲＳＡでは、数百桁におよぶ巨大な数の素数の積を用いて公開鍵と秘密鍵を生成する。このような素数から生成された一方の値から、他方を導き出すためには、巨大数の素因数分解が必要になる。この巨大数の素因数分解には膨大な計算処理が必要で、現実的な時間内に答えを出すことは不可能である。ここでは、鍵ペアの生成に、ＲＳＡアルゴリズムを利用しても、他の方法を利用しても良い。

【００６０】また、公開鍵暗号方式における「秘密鍵」は、そのデータの発信者が、間違いなく本人であることを証明する「電子署名」としても利用することができる。上述したように、通常の暗号化では、受信先が発行した公開鍵でデータを暗号化するが、電子署名では、発信元が送信するデータ（通常は、データにハッシュをかけた値）を自分の秘密鍵で暗号化して電子署名とし、データに付加して相手に送る。これを受け取った相手は、その送信元が発行した公開鍵を使って、電子署名の復号を行う。そして、受信したデータ（データのハッシュ値）と、電子署名を復号したデータを比較して、一致すれば、間違いなく本人が発信した情報であり、改竄されていないことが証明される。ここでは、受信先の公開鍵でデータを暗号化し、送信元の電子署名用の秘密鍵で電子署名を施したデータを送受信するものとする。

【００６１】ただし、公開鍵暗号方式では、その公開鍵が本当に本人のものであるか否かが照明されていなければならない。そこで、第三者機関が公的に本人認証を行うためのＰＫＩ（Public Key Infrastructure）が利用される。

【００６２】ＰＫＩでは、認証局（ＣＡ：Certification Authority）という信頼できる認証機関を設けて、電子署名による「電子証明書」とともに公開鍵を発行して、管理し、データの授受先の正当性（本人であること）を証明する仕組みを提供する。これにより、データ

の盗聴および改ざん、あるいは、なりすましを防止することができる。

【００６３】ライセンスサーバ３と登録済みのユーザが保有するパーソナルコンピュータ１－１乃至１－ｎは、お互いの公開鍵を交換する。そして、ライセンスサーバ３は、登録済みのユーザが保有するパーソナルコンピュータ１－１乃至１－ｎのうちのいずれかから、暗号化され、署名されたライセンス取得要求情報を受信する。ライセンス取得要求情報には、送信元ユーザ（ライセンス要求元）のユーザＩＤ、ライセンスの取得を要求するコンテンツのコンテンツＩＤ、および、そのコンテンツに付随しているフィールドに記載されたユーザ情報が添付される。

【００６４】ライセンス取得要求情報を受信したライセンスサーバ３は、ライセンス情報データベース１２から、ライセンステーブルを参照して、コンテンツＩＤに対応するライセンスキー（コンテンツに対する復号鍵）を検索し、例えば、ユーザＩＤなど、ライセンス供給先を特定するための情報を含むユーザ情報を生成して、ライセンスサーバの公開鍵で暗号化し、ライセンスステータス情報、制限情報などを付加して、ライセンスを生成する。ライセンスサーバ３は、ライセンスを暗号化し、電子署名を施した後、インターネット２を介して、ライセンス取得要求情報の送信元に送信する。ライセンステーブルについては後述する。

【００６５】そして、ライセンスサーバ３は、ライセンス情報データベース１２のライセンス発行テーブルに、ライセンス発行の履歴を記録し、ライセンス取得要求情報に添付されている情報を基に、コンテンツデータがどのようなユーザを経由して流通しているかを示す情報（以下、トレーシング情報と称する）を抽出して、ライセンス情報データベース１２のトレーシング情報テーブルに記録する。ライセンス発行テーブル、およびトレーシング情報テーブルについては後述する。

【００６６】以下、パーソナルコンピュータ１－１乃至パーソナルコンピュータ１－ｎを個々に区別する必要がない場合、単にパーソナルコンピュータ１と総称する。

【００６７】図３は、パーソナルコンピュータ１の構成を示すブロック図である。

【００６８】ＣＰＵ（Central Processing Unit）２１は、入出力インターフェース２２および内部バス２３を介して、ユーザが、入力部２４を用いて入力した各種指令に対応する信号や、ネットワークインターフェース３０を介して、例えば、ライセンスサーバ３などが送信した信号の入力を受け、入力された信号に基づいた各種処理を実行する。ＲＯＭ（Read Only Memory）２５は、ＣＰＵ２１が使用するプログラムや演算用のパラメータのうちの基本的に固定のデータを格納する。ＲＡＭ（Random Access Memory）２６は、ＣＰＵ２１の実行において使用するプログラムや、その実行において適宜変化するパラメータを格納する。ＣＰＵ２１、ＲＯＭ２５、およびＲＡＭ２６は、内部バス２３により相互に接続されている。

【００６９】内部バス２３は、入出力インターフェース２２とも接続されている。入力部２４は、例えば、キーボード、タッチパッド、ジョグダイヤル、あるいはマウスなどからなり、ユーザがＣＰＵ２１に各種の指令を入力するとき操作される。出力部２７は、例えば、ＣＲＴ（Cathode Ray Tube）や液晶表示装置などで構成される、各種情報をテキスト、あるいはイメージなどで表示する表示部や、音声を出力するスピーカ、更に、必要に応じて、音を発生するブザーや、点灯、もしくは消灯によりユーザに情報を伝達するためのＬＥＤランプなどで構成される。

【００７０】ＨＤＤ（hard disk drive）２８は、ハードディスクを駆動し、それらにＣＰＵ２１によって実行するプログラムや情報（例えば、コンテンツデータ）を記録または再生させる。ドライブ２９には、必要に応じて磁気ディスク３１、光ディスク３２、光磁気ディスク３３、および半導体メモリ３４が装着され、データの授受を行う。

【００７１】ネットワークインターフェース３０は、インターネット２と接続され、インターネット２を介して、ライセンスサーバ３などと情報の授受を行う。また、ネットワークインターフェース３０は、例えば、コンテンツデータを記憶している外部の記憶装置と接続されていても良い。

【００７２】これらの入力部２４乃至ネットワークインターフェース３０は、入出力インターフェース２２および内部バス２３を介してＣＰＵ２１に接続されている。

【００７３】なお、ライセンスサーバ３乃至決済サーバ５も、基本的に、パーソナルコンピュータ１と同様の構成を有するものであるので、そのハードウェアに関する詳細な説明は省略する。

【００７４】図４は、パーソナルコンピュータ１を利用するユーザのユーザ登録を実行し、パーソナルコンピュータ１が記録しているコンテンツデータを再生するための通常ライセンス、もしくはプレビューライセンスを発行するライセンスサーバ３の機能を示す機能ブロック図である。

【００７５】制御部４１は、インターネット２および入出力インターフェース４２を介して入力された、パーソナルコンピュータ１から送信された各種情報を基に、ライセンスサーバ３の動作を制御するものである。制御部４１は、例えば、パーソナルコンピュータ１から送信されたユーザの登録情報などをユーザ登録データベース１１に登録したり、新たに登録されたユーザが保有するパーソナルコンピュータ１に、メモリ４３に記録されている、ライセンスサーバ３の公開鍵や、コンテンツ復号アプリケーションプログラムなどを送信したり、ライセン

ス取得要求を受けて、対応するコンテンツのライセンスを生成し、要求元のパーソナルコンピュータ１に送信する処理を制御する。

【００７６】入出力インターフェース４２は、ライセンスサーバ３が、ユーザ登録データベース１１、ライセンス情報データベース１２、および、インターネット２と情報の授受を行うためのインターフェースである。

【００７７】メモリ４３には、ライセンスサーバ３の公開鍵や、コンテンツ復号アプリケーションプログラムなどの、パーソナルコンピュータ１に送信される情報や、制御部４１の処理に必要な各種情報が記録されている。

【００７８】暗号化および復号処理部４４は、登録済みのユーザが有するパーソナルコンピュータ１との通信において、送信する情報を暗号化し、署名するとともに、受信した情報の署名を確認し、復号する処理や、ライセンスに添付するユーザ情報を暗号化したり、ライセンス取得要求情報に含まれているユーザ情報を復号する処理を実行する。また、暗号化および復号処理部４４は、その内部に、秘密鍵記録部５１を備え、暗号化および署名の確認に用いられる、ライセンスサーバ３の秘密鍵を保存している。

【００７９】トレーシングデータ解析部４５は、ライセンス取得要求情報に添付されているユーザ情報などを基に、ライセンス情報データベース１２のトレーシング情報テーブルに登録されるデータから、それぞれのコンテンツが、どのような経路でユーザに配信されたのであるかを解析し、解析結果を基に、コンテンツ配信事業に有益な、様々なデータを抽出する。

【００８０】次に、図５のフローチャートを参照して、ユーザ登録実行時のパーソナルコンピュータ１とライセンスサーバ３との処理について説明する。

【００８１】ステップＳ１において、パーソナルコンピュータ１のＣＰＵ２１は、入出力インターフェース２２および内部バス２３を介して、入力部２４から入力されたユーザの操作を示す信号に従って、内部バス２３、入出力インターフェース２２、ネットワークインターフェース３０、およびインターネット２を介して、ライセンスサーバ３にアクセスする。パーソナルコンピュータ１のＣＰＵ２１は、例えば、ウェブブラウザを起動し、ライセンスサーバ３が公開しているウェブページにアクセスするようにしても良い。

【００８２】ステップＳ２において、パーソナルコンピュータ１のＣＰＵ２１は、ユーザ登録情報およびユーザの公開鍵（データ暗号化用および署名復号用）を、ライセンスサーバ３に送信する。ここでは、ユーザの公開鍵をライセンスサーバ３に送信するものとして説明したが、例えば、公開鍵を一般に公開するような場合は、公開鍵の入手方法についての情報をライセンスサーバ３に送信するようにしても良い。

【００８３】ステップＳ３において、ライセンスサーバ３の制御部４１は、インターネット２および入出力インターフェース４２を介して、ユーザ登録情報およびユーザの公開鍵（もしくは公開鍵の入手方法についての情報）を受信し、新たに登録するユーザのためのユーザＩＤを設定する。

【００８４】ステップＳ４において、ライセンスサーバ３の制御部４１は、設定されたユーザＩＤとともに、ユーザ登録情報およびユーザの公開鍵を、入出力インターフェース４２を介して、ユーザ登録データベース１１に登録する。

【００８５】ユーザ登録データベース１１には、図６に示されるユーザ登録管理テーブルが登録されている。ユーザ登録管理テーブルには、ライセンスサーバ３が発行したユーザＩＤ毎に、例えば、上述した公開鍵暗号方式を用いて情報を授受するためのユーザの公開鍵、ライセンスの送信先として登録されるメールアドレスに加えて、必要に応じて、ユーザの個人情報（ユーザの嗜好情報などを含む）などが登録される。

【００８６】ステップＳ５において、ライセンスサーバ３の制御部４１は、コンテンツ復号アプリケーションプログラムをメモリ４３から読み出し、入出力インターフェース４２およびインターネット２を介して、パーソナルコンピュータ１に送信する。コンテンツ復号アプリケーションプログラムとは、パーソナルコンピュータ１において、ライセンス取得要求情報を生成して送信したり、ライセンス取得時に、コンテンツに付随しているフィールドに記載されているユーザ情報の書き換え処理を実行したり、コンテンツデータを取得したライセンスで復号する処理を実行するアプリケーションであり、その詳細については後述する。

【００８７】ステップＳ６において、パーソナルコンピュータ１のＣＰＵ２１は、コンテンツ復号アプリケーションプログラムを受信し、インストールする。すなわち、ＣＰＵ２１は、コンテンツ復号アプリケーションプログラムをＨＤＤ２８に記録し、ＣＰＵ２１の制御に従って、ＲＡＭ２６にロードして実行することができるような状態にする。

【００８８】ステップＳ７において、ライセンスサーバ３の制御部４１は、ライセンスサーバ３の公開鍵（データ暗号化用および署名復号用）、およびステップＳ３において設定されたユーザＩＤを、入出力インターフェース４２およびインターネット２を介して、パーソナルコンピュータ１に送信する。

【００８９】ステップＳ８において、パーソナルコンピュータ１のＣＰＵ２１は、ライセンスサーバの公開鍵、およびユーザＩＤを受信し、ＨＤＤ２８に記録して、処理が終了する。

【００９０】以上説明した登録処理により、登録ユーザに対して、ユーザ毎に固有の番号であるユーザＩＤが設定されて、ライセンスサーバ３およびパーソナルコンピ

ュータ１の両方で記録される。そして、公開鍵暗号方式による情報の授受を行うために、ライセンスサーバ３は、自分自身の秘密鍵を保存しているとともに、公開鍵を登録済みのユーザに公開（登録済みのユーザが有するパーソナルコンピュータ１に送信）し、登録済みのユーザは、自分自身が有するパーソナルコンピュータ１に秘密鍵を保存するとともに、公開鍵をライセンスサーバ３に公開する。

【００９１】また、図５においては、ライセンスサーバ３が、ユーザＩＤを設定するものとして説明しているが、例えば、既にユーザに提供されている他のサービスのユーザＩＤや、携帯型電話機などの機器に個別に割り当てられている機器ＩＤなどを流用するようにしても、それらのＩＤがユーザに対して個別に割り当てられていればかまわない。

【００９２】図７は、図５のステップＳ６で受信し、インストールしたコンテンツ復号アプリケーションプログラムが起動している場合の、パーソナルコンピュータ１の機能ブロック図である。

【００９３】制御部６１は、入力部２４を用いてユーザが行った操作入力に従って、コンテンツ復号アプリケーションプログラムの動作を制御するものである。制御部６１は、例えば、暗号化および復号処理部６４の処理により暗号化され、電子署名が記載されたライセンス取得要求情報を、入出力インターフェース６２およびインターネット２を介して、ライセンスサーバ３に送信したり、コンテンツサーバ４から受信したコンテンツデータを、コンテンツデータベース６６に保存し、コンテンツ管理テーブル６７を更新する処理を制御する。

【００９４】入出力インターフェース６２は、パーソナルコンピュータ１が、インターネット２を介して、ライセンスサーバ３乃至決済サーバ５と情報の授受を行うためのインターフェースである。

【００９５】メモリ６３は、ＨＤＤ２８、ＲＯＭ２５、もしくはＲＡＭ２６に対応する。メモリ６３には、図５のステップＳ８において記録されたライセンスサーバ３の公開鍵および登録時に発行されたユーザＩＤ、並びに課金処理に必要となる個人情報とともに、制御部６１の処理に必要な各種情報が記録されている。

【００９６】暗号化および復号処理部６４は、ライセンスサーバ３との通信において、送信する情報を暗号化し、署名するとともに、受信した情報の署名を確認し、復号する処理や、ライセンスサーバ３から配布されたライセンスを用いて、コンテンツデータを復号する処理を実行する。また、暗号化および復号処理部６４は、その内部に、秘密鍵記録部７１を備え、暗号化および署名の確認に用いられる、ユーザの秘密鍵を保存している。

【００９７】再生処理部６５は、暗号化および復号処理部６４で復号されたコンテンツデータの入力を受け、所定のフォーマットに従って、データ伸長処理、エラー訂正処理、各種画像処理、あるいは音声データのD/A変換処理などの必要な処理を実行して、画像データは出力部２７の表示部７２に、音声データは出力部２７のスピーカ７３に、それぞれ出力する。

【００９８】コンテンツデータベース６６は、コンテンツサーバ４からダウンロードした、暗号化されたコンテンツデータを記録している。コンテンツ管理テーブル６７には、ダウンロードしたコンテンツのコンテンツＩＤ、コンテンツが記録されているアドレス情報、およびライセンスの有無やライセンスＩＤを記録している図１１を用いて後述するコンテンツ管理テーブルとともに、ライセンスサーバ３から受信したライセンスに含まれるライセンスキーが保存されている。

【００９９】次に、図８および図９のフローチャートを参照して、登録済みのユーザが保有しているパーソナルコンピュータ１において、図７を用いて説明したコンテンツ復号アプリケーションプログラムがＲＡＭ２６にロードされ、ＣＰＵ２１において実行されている場合の処理について説明する。

【０１００】ステップＳ２１において、制御部６１は、インターネット２および入出力インターフェース６２を介して、コンテンツサーバ４から、所望のコンテンツをダウンロードし、コンテンツデータベース６６に保存するとともに、コンテンツ管理テーブル６７に記録されている情報を更新する。制御部６１は、例えば、ウェブブラウザを起動し、コンテンツサーバ４が公開しているウェブページ（ダウンロードサイト）にアクセスし、所定の操作を実行して、所望のコンテンツデータをダウンロードするようにしても良い。

【０１０１】コンテンツは暗号化されており、通信経路上で、悪意ある第三者にデータを盗まれるようなことがあっても、対応するライセンスがなければ、コンテンツを再生することは出来ない。従って、コンテンツサーバ４とパーソナルコンピュータ１－１とのコンテンツデータの送受信は、上述した公開鍵暗号方式を用いずに実行される（図１０の図中ａ）。図１０においては、インターネット２は図示されていないが、情報の授受は、インターネット２を介して実行されている。

【０１０２】また、図１０の図中ｂに示されるように、コンテンツサーバ４からダウンロードされるコンテンツデータに添付しているフィールドには、このコンテンツデータがコンテンツサーバ４からダウンロードされたデータであることを示すユーザ情報（図中、ｃｏｎ－ｓｅｒｖｅｒ’と記載されている情報）が記載されている。ユーザ情報は、ライセンスサーバ３の公開鍵で暗号化されているので、ライセンスサーバ３の暗号化および復号処理部４４でしか復号されることはない。

【０１０３】また、ユーザ情報が、ライセンスサーバ３の公開鍵で暗号化され、ライセンスサーバ３においてのみ読み取りが可能であることを利用して、ユーザ情報

に、例えば、ライセンスの発行日時を示す情報や、コンテンツおよびライセンスの発行サービスに関する情報を付加することも可能である。

【０１０４】そして、制御部６１は、コンテンツ管理テーブル６７を用いて、ダウンロードされて、コンテンツデータベース６６に記録されている、暗号化されたコンテンツデータおよびそれぞれのコンテンツに対応するライセンスを管理する。

【０１０５】図１１を用いて、コンテンツ管理テーブル６７に登録される情報について説明する。コンテンツ管理テーブル６７には、コンテンツデータベース６６に保存されているコンテンツを表す固有のＩＤであるコンテンツＩＤ、コンテンツデータベース６６内で、コンテンツを記録している場所を示すアドレス情報、および対応するコンテンツを再生する場合に利用される、通常ライセンス用のライセンスＩＤと、プレビューライセンス用のライセンスＩＤが登録されている。ライセンスの発行要求をまだ行っていないコンテンツについては、もちろん、ライセンスＩＤは登録されておらず、コンテンツによっては、通常ライセンス用のライセンスＩＤと、プレビューライセンス用のライセンスＩＤのいずれか一方のみが登録されている場合もある。

【０１０６】ステップＳ２２において、制御部６１は、入力部２４から入力されるユーザの操作を示す信号を基に、ユーザから、プレビュー再生用のライセンス取得を指令する入力を受けたか否かを判断する。ステップＳ２２において、プレビュー再生用のライセンス取得を指令する入力を受けていないと判断された場合、処理は、ステップＳ２７に進む。

【０１０７】ステップＳ２２において、プレビュー再生用のライセンス取得を指令する入力を受けたと判断された場合、ステップＳ２３において、制御部６１は、対応するコンテンツのコンテンツＩＤと、自分自身のユーザＩＤ、およびそのコンテンツに付加されているユーザ情報（例えば、コンテンツサーバ４を示す情報（ｃｏｎ－ｓｅｒｖｅｒ）を含むユーザ情報）を添付したプレビューライセンス得要求情報を生成する。

【０１０８】ステップＳ２４において、制御部６１は、ステップＳ２３において生成したプレビューライセンス取得要求情報、およびメモリ６３に記録されているライセンスサーバ３の公開鍵を、暗号化および復号処理部６４に出力する。暗号化および復号処理部６４は、プレビューライセンス取得要求情報をライセンスサーバ３の公開鍵で暗号化する。

【０１０９】ステップＳ２５において、暗号化および復号処理部６４は、秘密鍵記録部７１に記録されている自分自身の署名用の秘密鍵を用いて、プレビューライセンス取得要求情報に電子署名を施す。

【０１１０】ステップＳ２６において、制御部６１は、暗号化および復号処理部６４によって暗号化され、電子署名されたプレビューライセンス取得要求情報を、図１０の図中ｃに示されるように、インターネット２を介して、ライセンスサーバ３に送信する。ライセンスサーバ３に送信されるプレビューライセンス取得要求情報には、図１０の図中ｄに示されるように、このコンテンツデータがコンテンツサーバ４からダウンロードされたデータであることを示すユーザ情報（図中、ｃｏｎ－ｓｅｒｖｅｒ’と記載されている情報）、自分自身のユーザＩＤ（図中、ａ１１１１１１１と記載されている情報）、およびコンテンツＩＤ（図中、××××と記載されている情報）が、少なくとも記載されている。

【０１１１】ここで、ライセンスサーバ３は、プレビューライセンス発行のための条件が満たされているか否かを判断し、条件が満たされている場合、プレビューライセンスを発行する（後述する図１５および図１６のステップＳ６６乃至ステップＳ６８、およびステップＳ７３乃至ステップＳ７６の処理）。

【０１１２】ステップＳ２２において、プレビュー再生用のライセンス取得を指令する入力を受けていないと判断された場合、ステップＳ２７において、制御部６１は、入力部２４から入力されるユーザの操作を示す信号を基に、ユーザから、通常再生用のライセンス取得を指令する入力を受けたか否かを判断する。ステップＳ２７において、通常再生用のライセンス取得を指令する入力を受けていないと判断された場合、処理は、ステップＳ２２に戻り、それ以降の処理が繰り返される。

【０１１３】ステップＳ２７において、通常再生用のライセンス取得を指令する入力を受けたと判断された場合、ステップＳ２８において、制御部６１は、対応するコンテンツのコンテンツＩＤ、自分自身のユーザＩＤ、および、そのコンテンツに付加されているユーザ情報を添付した通常ライセンス取得要求情報を生成する。

【０１１４】ステップＳ２９において、制御部６１は、ステップＳ２８において生成した通常ライセンス取得要求情報、およびメモリ６３に記録されているライセンスサーバ３の公開鍵を、暗号化および復号処理部６４に出力する。暗号化および復号処理部６４は、通常ライセンス取得要求情報をライセンスサーバ３の公開鍵で暗号化する。

【０１１５】ステップＳ３０において、暗号化および復号処理部６４は、秘密鍵記録部７１に記録されている自分自身の署名用の秘密鍵を用いて、通常ライセンス取得要求情報に電子署名を施す。

【０１１６】ステップＳ３１において、制御部６１は、暗号化および復号処理部６４によって暗号化され、電子署名された通常ライセンス取得要求情報を、ステップＳ２６において説明した場合と同様に、図１０の図中ｃに示されるように、インターネット２を介して、ライセンスサーバ３に送信する。ライセンスサーバ３に送信されるプレビューライセンス取得要求情報にも、ステップＳ

２６において説明した場合と同様に、図１０の図中ｄに示されるように、このコンテンツデータがコンテンツサーバ４からダウンロードされたデータであることを示すユーザ情報が記載されている。

【０１１７】ここで、ライセンスサーバ３は、課金処理に関する指示を、パーソナルコンピュータ１および決済サーバ５に送信する（後述する図１６のステップＳ６９の処理）。

【０１１８】ステップＳ３２において、制御部６１は、図１２の図中ｅに示されるように、課金処理に関する指示を、インターネット２および入出力インターフェース６２を介して、ライセンスサーバ５から受信する。ここで、課金処理に関する指示を示す情報は、必要に応じて、ライセンスと同様に、ユーザの公開鍵で暗号化され、ライセンスサーバ３の秘密鍵で署名されていても良いし、他の方法を用いて、情報が安全に送信されるようにしても良い。

【０１１９】ステップＳ３３において、制御部６１は、必要に応じて、暗号化および復号処理部６４の処理により、受信した情報の署名を確認し、復号した後、課金処理に関する指示に従って、図１２の図中ｆに示されるように、決済サーバ５にアクセスし、課金処理を実行する。

【０１２０】ここで、決済サーバ５は、ユーザとの課金処理が正しく実行された場合、ライセンスサーバ３に通常ライセンスの発行リクエストを通知する。そして、ライセンスサーバ３は、課金処理をはじめとする通常ライセンス発行のための条件が満たされているか否かを判断し、条件が満たされている場合、通常ライセンスを発行する（後述する図１６のステップＳ７０乃至ステップＳ７６の処理）。

【０１２１】ステップＳ２６の処理の終了後、もしくは、ステップＳ３３の処理の終了後、ステップＳ３４において、制御部６１は、図１３の図中ｈに示されるように、ライセンスサーバ３の署名用の秘密鍵で電子署名され、ユーザの公開鍵で暗号化されたデータ（すなわち、ライセンス）を、インターネット２および入出力インターフェース６２を介して、ライセンスサーバ３から受信する。

【０１２２】ライセンスには、図１３の図中ｇで示されるように、ライセンスが通常ライセンスであるか、プレビューライセンスであるかを示すライセンスステータス、コンテンツを復号するためのライセンスキー、再生回数や、再生時間などの制限情報、およびライセンスサーバの公開鍵で暗号化されているユーザ情報が含まれている。ライセンスに含まれているユーザ情報には、ライセンスを受けるユーザを示す情報（例えば、そのユーザのユーザＩＤなど）が含まれている。

【０１２３】このユーザ情報は、コンテンツとともに、ピアツーピアで授受される情報であるので、第三者にユーザを示す情報を盗まれないように、ライセンスサーバの公開鍵で暗号化されているが、ユーザ情報が、例えば、ユーザＩＤのみで構成されている場合には、暗号化されたデータが毎回同じ値となってしまう。そのため、ユーザＩＤなどのユーザを特定するための情報以外に、例えば、日時や、サービスに関する情報などの他の情報をユーザ情報に含ませることにより、暗号化されたユーザ情報の値をライセンス毎に変更し、ユーザ情報を第三者に悪用されることを防ぐことが可能である。

【０１２４】ステップＳ３５において、暗号化および復号処理部６４は、受信したデータに対して、メモリ６３に保存されているライセンスサーバ３の署名用の公開鍵を用いて署名を確認する。

【０１２５】ステップＳ３６において、制御部６１は、暗号化および復号処理部６４が実行した署名を確認する処理の結果を受け、受信したデータの送信元は、間違いなくライセンスサーバ３であるか否かを判断する。

【０１２６】ステップＳ３６において、受信したデータの送信元はライセンスサーバ３であると判断された場合、ステップＳ３７において、制御部６１は、暗号化および復号処理部６４を制御して、秘密鍵記録部７１に記録されているユーザの秘密鍵で、受信したデータを復号させる。

【０１２７】ステップＳ３８において、制御部６１は、ステップＳ３７において、暗号化および復号処理部６４は、受信したデータを正しく復号できたか否かを判断する。

【０１２８】ステップＳ３６において、受信したデータの送信元はライセンスサーバ３ではないと判断された場合、もしくは、ステップＳ３８において、受信したデータを正しく復号できなかったと判断された場合、ステップＳ３９において、制御部６１は、出力部２７の表示部７２に、エラーメッセージを表示して、処理が終了する。

【０１２９】ステップＳ３８において、受信したデータを正しく復号できたと判断された場合、ステップＳ４０において、制御部６１は、復号したライセンスに含まれるユーザ情報を抽出し、図１３の図中ｉに示されるように、対応するコンテンツのユーザ情報と書き換える（上書きする）。従って、ライセンス取得済みのコンテンツに添付されているフィールドに記載されているユーザ情報は、自分自身を示す情報（例えば、ユーザＩＤ）を含むユーザ情報となる。

【０１３０】ステップＳ４１において、制御部６１は、復号されたライセンス（通常ライセンス、もしくはプレビューライセンス）をコンテンツ管理テーブル６７に保存する。そして、制御部６１は、入力部２４から入力されるユーザの操作に従って、必要に応じて、暗号化および復号処理部６４に、コンテンツ管理テーブル６７に保存されているライセンスのライセンスキーを用いてコン

テンツを復号させ、再生処理部６５を制御して、復号されたコンテンツを再生させる。再生されたコンテンツのうち、画像データは、出力部２７の表示部７２に出力されて表示され、音声データは、出力部２７のスピーカ２７に出力され、音声出力される。

【０１３１】ここで、ダウンロードされたコンテンツデータは、暗号化された状態でコンテンツデータベース６６に保存される。すなわち、ライセンスキーで復号されたコンテンツを記録しておくことができないため、再生処理のたびに、ライセンスキーを用いて復号処理が実行される。これにより、ライセンスに、再生回数の制限が含まれている場合、不当な回数の再生処理を未然に防ぐことができる。

【０１３２】コンテンツの再生回数が制限されている場合、所定の回数を再生したユーザは、新たに、通常ライセンスをライセンスサーバ３に要求して、対応するコンテンツを再生する。この場合、もちろん、コンテンツデータを再ダウンロードする必要はないので、コンテンツデータ自身に再生回数の規制がなされて配信される場合と比較して、ユーザは、コンテンツデータのダウンロードのためにインターネット２に接続する時間を少なくすることができる。そして、コンテンツ配信サービス事業者は、ライセンスの再供給により、不当な回数の再生処理を未然に防ぎつつ、コンテンツデータの配信に対して、正当な報酬を得ることができる。

【０１３３】次に、ステップＳ４２において、制御部６１は、他のパーソナルコンピュータから、ピアツーピアでのコンテンツデータのコピーを要求されたか否かを判断する。例えば、図１３のパーソナルコンピュータ１－１は、図１３の図中ｊに示されるように、ライセンスサーバに登録済みであるパーソナルコンピュータ１－２からコンテンツデータのコピーを要求されたか否かを判断する。

【０１３４】ステップＳ４２において、他のパーソナルコンピュータから、ピアツーピアでのコンテンツデータのコピーを要求されたと判断された場合、ステップＳ４３において、制御部６１は、自分自身を示すユーザ情報が付加されたコンテンツデータを、図中ｋに示されるように、要求元のパーソナルコンピュータに送信して、処理が終了される。ステップＳ４２において、他のパーソナルコンピュータ１から、ピアツーピアでのコンテンツデータのコピーを要求されていないと判断された場合、処理が終了される。

【０１３５】パーソナルコンピュータ１－２は、パーソナルコンピュータ１－１のユーザ情報が付加されたコンテンツデータ（図１３の図中ｉに示されるコンテンツデータ）を受信する。その後、パーソナルコンピュータ１－２は、図１４の図中ｌに示されるように、コンテンツＩＤ、自分自身のユーザＩＤ、および、パーソナルコンピュータ１－１のユーザ情報が付加されたライセンス取得要求情報を、ライセンスサーバ３の公開鍵で暗号化し、パーソナルコンピュータ１－２を保有しているユーザの署名用の秘密鍵で署名して、ライセンスサーバ３に送信することができる（図１４の図中ｍ）。

【０１３６】ライセンスサーバ３は、上述した所定の処理を実行し、パーソナルコンピュータ１－２を保有しているユーザの公開鍵で暗号化し、ライセンスサーバ３の署名用の秘密鍵で署名したライセンスを、パーソナルコンピュータ１－２に送信する（図１４の図中ｎ）。このライセンスには、図中ｏに示されるように、ライセンスステータス、ライセンスキー、制限情報、およびパーソナルコンピュータ１－２を保有しているユーザを示す情報（例えば、ユーザＩＤなど）を含むユーザ情報を含んでいる。ライセンスを受信したパーソナルコンピュータ１－２は、自分自身に保存されているコンテンツデータに付加されているフィールドに記載されているユーザ情報を、受信したライセンスに含まれていた自分自身のユーザ情報に書き換える（図１４の図中ｐ）。

【０１３７】なお、パーソナルコンピュータ１を利用するユーザが、決済サーバ５に対して、図５を用いて説明したライセンスサーバ３への登録処理と同様の処理を実行して登録処理を行うようにし、決済サーバ５と、パーソナルコンピュータ１とが、暗号化された情報をやり取りするようにしても良いことはもちろんである。

【０１３８】図８および図９を用いて説明した処理においては、ステップＳ３３において、決済サーバ５とパーソナルコンピュータ１とで実行される課金処理を、ライセンスサーバ３に対する通常ライセンス取得要求やライセンスの送受信と独立して実行されるものとして説明したが、例えば、パーソナルコンピュータ１からライセンスサーバ３へ、通常ライセンス取得要求情報を送信する代わりに、パーソナルコンピュータ１は、通常ライセンス取得要求情報を決済サーバ５に送信し、決済サーバ５が、課金処理の終了後、通常ライセンス取得要求情報を、課金処理を実行したユーザのユーザＩＤとともに、ライセンスサーバ３に送信するようにしてもよい。この場合、ライセンスサーバ３は、決済サーバ５から送信された通常ライセンス取得要求情報以外は受理しないものとすることができる。

【０１３９】次に、図１５および図１６を参照して、図８および図９を用いて説明したパーソナルコンピュータ１の処理と並行して実行されるライセンスサーバ３の処理について説明する。ここでは、ユーザ情報に含まれる、ユーザを特定するための情報は、ユーザＩＤであるものとして説明する。

【０１４０】ステップＳ６１において、ライセンスサーバ３の制御部４１は、パーソナルコンピュータ１を有するユーザの秘密鍵で電子署名され、ライセンスサーバ３の公開鍵で暗号化されたデータ（図１０の図中ｃ、もしくは図１４の図中ｍで示されるデータ）を、インターネ

ット２および入出力インターフェース４２を介して受信する。

【０１４１】ステップＳ６２において、制御部４１は、例えば、データの送信者のアドレスなどを検索キーとして、ユーザ登録データベース１１に登録されているユーザの公開鍵を検索し、暗号化および復号処理部４４にステップＳ６１において受信したデータとともに供給して、検索されたユーザの署名用の公開鍵で電子署名を確認する。

【０１４２】ステップＳ６３において、制御部４１は、ステップＳ６２において復号処理が実行できたか否かを基に、受信したデータの送信元は、登録されているユーザのパーソナルコンピュータ１であるか否かを判断する。

【０１４３】ステップＳ６３において、受信したデータの送信元は、登録されているユーザのパーソナルコンピュータ１ではないと判断された場合、処理は、後述するステップＳ７８に進む。

【０１４４】ステップＳ６３において、受信したデータの送信元は、登録されているユーザのパーソナルコンピュータ１であると判断された場合、ステップＳ６４において、制御部４１は、暗号化および復号処理部４４に、秘密鍵記録部５１に記録されているライセンスサーバ３の秘密鍵を用いて、受信したデータを復号させる。

【０１４５】ステップＳ６５において、制御部４１は、ステップＳ６４において復号された受信データは、プレビューライセンス取得要求情報であるか否かを判断する。ステップＳ６５において、受信データは、プレビューライセンス取得要求情報ではないと判断された場合、処理は、後述するステップＳ６９に進む。

【０１４６】ステップＳ６５において、受信データは、プレビューライセンス取得要求情報であると判断された場合、ステップＳ６６において、制御部４１は、プレビューライセンス発行のための条件が満たされているか否かを判断する。例えば、制御部４１は、復号されたプレビューライセンス取得要求情報と、ユーザ登録データベース１１の登録内容に不一致点がないか（例えば、パスワードを必要としている場合に、パスワードが誤って記載されていないか、など）を確認したり、プレビューライセンスの発行が、１つのコンテンツに１回だけ、もしくは所定の回数以下であると決められているような場合には、ライセンス情報データベース１２を参照して、対応するユーザのプレビューライセンスの発行履歴を確認して、所定回数以上のプレビューライセンス要求であるか否かを確認する。

【０１４７】ステップＳ６６において、プレビューライセンス発行のための条件が満たされていないと判断された場合、処理は、後述するステップＳ７８に進む。

【０１４８】ステップＳ６６において、プレビューライセンス発行のための条件が満たされていると判断された場合、ステップＳ６７において、制御部４１は、復号されたプレビューライセンス取得要求情報を基に、ライセンスを要求するコンテンツＩＤ、受信したライセンス取得要求情報のライセンス種別、ライセンス取得要求情報に添付されているユーザ情報に含まれるユーザＩＤ、およびライセンス要求元のユーザＩＤなどの、ライセンス要求に関する情報を、ライセンス情報データベース１２のトレーシング情報テーブルに登録する。

【０１４９】図１７に、トレーシング情報テーブルを示す。トレーシング情報テーブルには、ライセンス取得要求情報に添付されていたコンテンツＩＤ、ライセンスの種別を示すライセンスステータス、ユーザ情報に含まれているユーザＩＤ、すなわち、コンテンツの配信元のユーザＩＤ、およびライセンス取得要求情報を送信した配信先ユーザＩＤが登録されている。

【０１５０】ステップＳ６８において、制御部４１は、プレビューライセンスを要求されたコンテンツＩＤを基に、ライセンス情報データベース１２のライセンステーブルを参照して、要求されたコンテンツに対応するプレビュー再生用のライセンスキーを検索し、少なくともライセンス取得要求情報を送信したユーザのユーザＩＤを含むユーザ情報を生成し、必要に応じて、例えば、再生時間や、デグレードの内容（ビットレートや解像度情報）などの制限情報などを付加して、プレビューライセンスを生成して、処理は、後述するステップＳ７３に進む。

【０１５１】ライセンステーブルを図１８に示す。ライセンステーブルには、コンテンツＩＤ毎に、通常ライセンスとプレビューライセンスそれぞれのライセンスＩＤが記録され、必要に応じて、ライセンス情報データベース１２内に対応するライセンスが記録されている記録位置を示すアドレス情報が記録されている。

【０１５２】ステップＳ６５において、受信データはプレビューライセンス取得要求情報ではないと判断された場合、受信データは、通常ライセンス取得要求情報であるので、ステップＳ６９において、制御部４１は、課金処理に関する指示を、入出力インターフェース４２およびインターネット２を介して、通常ライセンス要求元であるパーソナルコンピュータ１および決済サーバ５に送信する。

【０１５３】ステップＳ７０において、制御部４１は、決済サーバ５から、対応するユーザＩＤに対して、指定されたコンテンツＩＤの通常ライセンスの発行リクエストが出されているか否か、すなわち、ユーザが、決済サーバ５との課金処理を正しく終了したか否かを判断する。

【０１５４】ステップＳ７０において、決済サーバ５から通常ライセンスの発行リクエストが出されていないと判断された場合、処理は、後述するステップＳ７８に進む。

【０１５５】ステップＳ７０において、決済サーバ５から通常ライセンスの発行リクエストが出されていると判断された場合、ステップＳ７１において、ステップＳ６７と同様の処理が実行される。

【０１５６】ステップＳ７２において、制御部４１は、通常ライセンスを要求されたコンテンツＩＤを基に、ライセンス情報データベース１２のライセンステーブルを参照して、要求されたコンテンツに対応する通常再生用のライセンスキーを検索し、少なくともライセンス取得要求情報を送信したユーザのユーザＩＤを含むユーザ情報を生成し、必要に応じて、例えば、再生回数やコピーガードなどの制限情報などを付加して、発行する通常ライセンスを生成する。

【０１５７】ステップＳ６８の処理の終了後、もしくは、ステップＳ７２の処理の終了後、ステップＳ７３において、制御部４１は、ユーザ登録データベース１１から、ライセンス要求元のユーザの公開鍵を検索して読み出し、暗号化および復号処理部４４に供給する。

【０１５８】ステップＳ７４において、制御部４１は、暗号化および復号処理部４４に生成したライセンス（ステップＳ６８において生成したプレビューライセンス、もしくは、ステップＳ７２において生成した通常ライセンス）を供給し、ステップＳ７３において検索された、対応するユーザの公開鍵で暗号化させる。

【０１５９】ステップＳ７５において、制御部４１は、暗号化および復号処理部４４を制御して、暗号化されたライセンスに、秘密鍵記録部５１に記録されているライセンスサーバ３の署名用の秘密鍵で電子署名を施させる。

【０１６０】ステップＳ７６において、制御部４１は、ユーザ登録データベース１１のユーザ登録管理テーブルに登録されているユーザの電子メールアドレスを参照して、暗号化され、電子署名を施されたライセンスを、入出力インターフェース４２およびインターネット２を介して、要求元のパーソナルコンピュータ１に送信する（図１３の図中ｈ、もしくは図１４の図中ｎで示されるデータ）。

【０１６１】ステップＳ７７において、制御部４１は、ライセンス情報データベース１２のライセンス発行テーブルを更新して、処理が終了される。

【０１６２】図１９にライセンス発行テーブルを示す。ライセンス発行テーブルには、ライセンスを発行したユーザＩＤ、ライセンスを発行したコンテンツＩＤ、発行したライセンスの種類を示すライセンスステータスが登録される。

【０１６３】ステップＳ６３において、受信したデータの送信元は、登録されているユーザのパーソナルコンピュータ１ではないと判断された場合、ステップＳ６６において、プレビューライセンス発行のための条件が満たされていないと判断された場合、もしくは、ステップＳ

７０において、決済サーバ５から通常ライセンスの発行リクエストが出されていないと判断された場合、ステップＳ７８において、制御部４１は、図示しない表示部にエラーメッセージを表示してライセンスサーバ３の管理者にエラーの発生を通達するとともに、必要に応じて、入出力インターフェース４２およびインターネット２を介して、パーソナルコンピュータ１にもエラーメッセージを返信して、処理が終了される。

【０１６４】以上説明した処理により、プレビューライセンス、もしくは通常ライセンスがライセンスサーバ３から、ユーザが保有するパーソナルコンピュータ１に送信されるので、ユーザは、コンテンツサーバ４、もしくは他のパーソナルコンピュータから受信したコンテンツデータを復号して再生することが可能となる。

【０１６５】そして、コンテンツは、ユーザ情報が添付された状態で、パーソナルコンピュータ１に授受される。ユーザ情報は、ライセンスサーバ３の公開鍵で暗号化されているので、ライセンスサーバ３のみ読み取ることができるようになされている。すなわち、ユーザＩＤなどを含むユーザ情報がコンテンツとともにピアツーピアで授受されて、悪意ある第三者に傍受された場合においても、悪用されることを防ぐことができる。

【０１６６】ユーザ情報は、ライセンス取得要求情報に含まれて、パーソナルコンピュータ１からライセンスサーバ３に送信される。パーソナルコンピュータ１は、ライセンスに含まれるユーザ情報を用いて、コンテンツに添付されているユーザ情報を上書きする。ライセンスサーバ３は、ライセンス取得要求情報に含まれるユーザ情報を基に、図１７を用いて説明したトレーシング情報テーブルや、図１９を用いて説明したライセンス発行テーブルを更新するので、図４を用いて説明したトレーシング情報解析部４５の処理により、コンテンツデータの流れをトレーシングすることが可能となる。

【０１６７】トレーシング情報解析部４５は、例えば、図１７を用いて説明したトレーシング情報テーブルを基に、コンテンツを他のユーザにピアツーピアで配信したユーザ（配信元ユーザ）に対して、例えば、ポイントなどを発行して、一定のポイントでプレゼントを贈ったり、通常ライセンス購入時にポイント分の料金を割引するなどのサービスを提供することが出来る。

【０１６８】また、配信先のユーザが通常ライセンスを要求したか、プレビューライセンスを要求したかによって、発行するポイントを変更したり、自分自身がプレビューライセンスを要求した後、通常ライセンスを要求することによって、自分自身が配信元ユーザとなる場合をポイント発行から除くことなども可能となる。

【０１６９】それに加えて、トレーシング情報解析部４５は、図１７を用いて説明したトレーシング情報テーブル、および図１９を用いて説明したライセンス発行テーブルを基に、ユーザの嗜好、コンテンツの配信能力、あ

るいは、プレビューの方法が的確であるか否かなどを、詳細に解析することが可能となる。

【０１７０】例えば、プレビューライセンスの要求数に対して、通常ライセンスの要求数が少ないようなコンテンツは、ユーザにとって、魅力がないコンテンツであるか、あるいは、プレビューの方法が良くない（例えば、再生箇所が的確でない、デグレードが強くて、コンテンツのよさが伝わり難いなど）という可能性がある。

【０１７１】それに対して、通常ライセンスの配信元ユーザＩＤが自分自身のユーザＩＤである場合、そのユーザは、プレビューライセンス要求後、通常ライセンスを要求している。そのような場合は、プレビューの方法は、的確であると考えることができる。更に、通常ライセンスの配信元ユーザＩＤが自分自身のユーザＩＤではない場合、そのユーザは、プレビューライセンスを要求せずに、通常ライセンスを要求しているので、対応するコンテンツは、ユーザにとって、非常に魅力的なタイトル、あるいはアーチストであり、プレビューなしでも購入を希望するものであると考えられる。

【０１７２】また、配信元ユーザＩＤがコンテンツサーバ４となっているコンテンツに対するライセンス要求を多く送信するユーザは、コンテンツサーバ４が公開しているウェブサイトなどをこまめにチェックし、コンテンツを多くダウンロードするユーザであるといえる。

【０１７３】更に、通常ライセンス要求に対して、その配信元ユーザＩＤと配信先ユーザＩＤが繰り返して同一のユーザＩＤである場合、そのコンテンツは、同一のユーザによって、１ライセンスの規定数以上繰り返し再生されているということであるから、コンテンツの満足度が非常に高いといえる。

【０１７４】また、あるコンテンツを、多くの他のユーザに配信するユーザは、対応するコンテンツを気に入ったので、友人等に広く勧めていると考えることができるので、コンテンツの配信状況から、ユーザの嗜好を推測することも可能となる。

【０１７５】更に、トレーシング情報テーブルにおいて、配信元ユーザとして多く登録されているユーザは、コンテンツの配信に積極的であるといえるが、例えば、あるコンテンツの通常ライセンスを要求していないユーザのユーザＩＤが、同一のコンテンツの他のユーザからのライセンス取得要求情報に多く添付されている、すなわち、トレーシング情報テーブルにおいて、配信元ユーザとして多く登録されているような場合、対応するユーザは、プレビューした結果、自分自身はあまり気に入らない場合であっても、そのコンテンツを気に入りそうなユーザに数多く配信している、すなわち、コンテンツを非常に積極的に広めようとしていることが分かる。

【０１７６】また、トレーシング情報テーブルにおいて、通常ライセンスに対する配信元ユーザとして多く登録されているユーザ、あるいは、通常ライセンスに対して配信元ユーザＩＤと配信先ユーザＩＤが同一である場合、そのコンテンツのプレビューライセンス要求時の配信元ユーザとして多く登録されているユーザは、他のユーザに対して的確にコンテンツを配信し、コンテンツの売上、すなわち通常ライセンスの要求数の向上に貢献していることが分かる。

【０１７７】トレーシング情報解析部４５は、上述した内容以外にも、トレーシング情報テーブル、およびライセンス発行テーブルに登録されたデータを基に、更に様々な情報を解析することができる。

【０１７８】以上説明したように、ユーザからライセンス要求が行われる毎に、ライセンスサーバ３に、トレーシング情報の基となるユーザ情報が送信されるので、コンテンツ配信サービス事業者は、ポイントの発行など、ピアツーピアでコンテンツを他のユーザに配信したユーザに対するサービスを速やかに提供することが可能となる。これにより、コンテンツの配信を更に行おうとするユーザの意欲が高まるので、コンテンツの流通を促進することが可能となる。

【０１７９】ここで、ユーザのパーソナルコンピュータ１において、ライセンス取得要求情報に、コンテンツに添付されていたユーザ情報を含ませる処理、および、受信したライセンスに添付されていた自分自身のユーザ情報を、コンテンツに添付されていたユーザ情報に上書きする処理は、要求するライセンスが、プレビューライセンスであっても、通常ライセンスであっても同様の処理である。すなわち、２種類のライセンスがあるにもかかわらず、パーソナルコンピュータ１の処理は、非常に簡単であるといえる。

【０１８０】そして、ライセンスサーバ３において、ユーザＩＤが添付されたのは、プレビューライセンス取得要求情報であるか、通常ライセンス取得要求情報であるかのライセンスステータスが登録され、コンテンツＩＤとともに、添付されたユーザ情報に含まれるコンテンツの配信元のユーザＩＤ、および、ライセンス取得要求情報の送信元のユーザＩＤ、すなわち、コンテンツの配信先のユーザＩＤが、トレーシング情報テーブルに登録される。そして、ライセンス発行時に、ライセンス発行テーブルに、ライセンス取得要求情報の送信元のユーザＩＤ、コンテンツＩＤ、およびライセンスステータスが登録されるようになされている。

【０１８１】そして、ライセンス発行サーバ３を管理する、例えば、コンテンツ配信サービス事業者は、トレーシング情報テーブルおよびライセンス発行テーブルに登録されている情報から、コンテンツの流通経路、コンテンツの満足度、プレビューの効果、ユーザの嗜好、あるいはユーザ個々のコンテンツ配信能力などについて、非常に詳細な情報を得ることができるので、これらの情報を活用して、コンテンツの販売を促進し、顧客満足度を向上することができる。

【０１８２】換言すれば、ユーザのパーソナルコンピュータ１において、ライセンス取得要求情報をライセンスサーバ３に送信する時に、ライセンスとは異なる経路で入手されるコンテンツデータに添付されているユーザ情報を送信し、かつ、コンテンツデータに添付されていたユーザＩＤを、受信したライセンスに添付されていた自分自身のユーザＩＤで上書きするという非常に簡単な処理が実行されることによって、ライセンスサーバ３を管理するコンテンツ配信サービス事業者は、コンテンツの流通経路、コンテンツの満足度、プレビューの効果、ユーザの嗜好、あるいはユーザ個々のコンテンツ配信能力などについて、非常に詳細な情報を得ることができる。

【０１８３】また、本発明によると、通常ライセンスが要求されたときのみならず、プレビューライセンスが要求されたときにも、コンテンツの配信元ユーザのユーザＩＤが登録されるので、コンテンツが購入されない（通常ライセンスが要求されない）場合においても、コンテンツのトレーシングが可能である。

【０１８４】以上説明した処理によれば、ユーザが利用しているパーソナルコンピュータ１において、ライセンス取得要求情報がライセンスサーバ３に送信され、ライセンスを受信した場合に、対応するコンテンツに添付されているフィールドに記載されているユーザ情報を、ライセンスに含まれているユーザ情報で上書きするものとして説明しているが、例えば、ライセンスサーバ３が、ライセンスにユーザ情報を添付せず、それぞれのパーソナルコンピュータ１において、自分自身のユーザＩＤをライセンスサーバ３の公開鍵で暗号化してユーザ情報を作成し、コンテンツに添付されているフィールドに上書きするようにしても良い。

【０１８５】その場合ライセンスサーバ３の制御部４１は、ライセンスステータス、ライセンスキーおよび制限情報から構成されるライセンスを、上述したように、ユーザの公開鍵で暗号化し、自分自身の署名用の秘密鍵で署名して、パーソナルコンピュータ１に送信する。

【０１８６】パーソナルコンピュータ１の制御部６１は、自分自身のユーザＩＤを、メモリ６３に保存しているライセンスサーバ３の公開鍵で暗号化したものを少なくとも含むユーザ情報を生成する。そして、ライセンス取得要求情報を送信したとき、もしくは、ライセンスを受信したとき、暗号化されたユーザ情報を、対応するコンテンツに添付されているフィールドに上書きする。そして、他のユーザが保有するパーソナルコンピュータに、ユーザ情報が添付されているコンテンツデータをピアツーピアで配信する。

【０１８７】そして、このコンテンツデータを受信したパーソナルコンピュータ１がライセンスサーバ３に送信するライセンス取得要求情報には、ライセンスサーバ３の公開鍵で暗号化されたユーザ情報が添付されているので、ライセンスサーバ３の制御部４１は、暗号化および

復号処理部４４を制御して、添付されているユーザ情報をライセンスサーバ３の秘密鍵を用いて復号し、トレーシング情報を得ることができる。

【０１８８】なお、ここでは、ユーザのパーソナルコンピュータ１とライセンスサーバ３とが授受するデータの暗号化および復号に用いる公開鍵と秘密鍵のペアと、電子署名に用いる公開鍵と秘密鍵のペアとを、それぞれ別のものとして説明したが、データの暗号化および復号用と、電子署名用の鍵のペアは、同一のものを利用するようにしても良い。

【０１８９】なお、ここでは、ユーザがダウンロードしたコンテンツを記録し、ライセンスキーを用いて復号して再生するためにパーソナルコンピュータ１を用いるものとして説明しているが、例えば、携帯型電話機、ＰＤＡ（Personal Digital Assistant）などの各種情報処理端末や、ＣＤ（Compact Disk）、ＤＶＤ（Digital Versatile Disk）、もしくはＭＤ（Mini-Disk）（商標）などのストレージデバイス、あるいは、内部に備えたハードディスクなどの記録媒体に記録されているコンテンツデータを再生することが可能な記録再生装置などにおいても、本発明は適応することが可能である。

【０１９０】上述した一連の処理は、ソフトウェアにより実行することもできる。そのソフトウェアは、そのソフトウェアを構成するプログラムが、専用のハードウェアに組み込まれているコンピュータ、または、各種のプログラムをインストールすることで、各種の機能を実行することが可能な、例えば汎用のパーソナルコンピュータなどに、記録媒体からインストールされる。

【０１９１】この記録媒体は、図３に示すように、コンピュータとは別に、ユーザにプログラムを提供するために配布される、プログラムが記録されている磁気ディスク３１（フレキシブルディスクを含む）、光ディスク３２（CD-ROM（Compact Disk-Read Only Memory），ＤＶＤ（Digital Versatile Disk）を含む）、光磁気ディスク３３（ＭＤ(Mini-Disk)（商標）を含む）、もしくは半導体メモリ３４などよりなるパッケージメディアなどにより構成される。

【０１９２】また、本明細書において、記録媒体に記録されるプログラムを記述するステップは、記載された順序に沿って時系列的に行われる処理はもちろん、必ずしも時系列的に処理されなくとも、並列的あるいは個別に実行される処理をも含むものである。

【０１９３】なお、本明細書において、システムとは、複数の装置により構成される装置全体を表すものである。

【０１９４】

【発明の効果】本発明の第１の情報処理装置および情報処理方法、並びにプログラムによれば、コンテンツを取得し、コンテンツに添付されている第１の情報、コンテンツを特定するための第２の情報、および自分自身を特

定することができる第３の情報を含む第４の情報を生成し、生成された第４の情報を送信し、コンテンツを再生するために必要な第５の情報を受信し、第５の情報に添付されている第６の情報を抽出し、抽出された第６の情報を、コンテンツに添付されている第１の情報に代わって、コンテンツに添付するようにしたので、コンテンツを再生するためのいわゆるライセンスの供給を受けるとともに、コンテンツの流通に関する情報をトレーシングするための情報をライセンスの供給者に送信することができる。

【０１９５】本発明の第２の情報処理装置および情報処理方法、並びにプログラムによれば、コンテンツを取得し、コンテンツに添付されている第１の情報、コンテンツを特定するための第２の情報、および自分自身を特定することができる第３の情報を含む第４の情報を生成し、生成された第４の情報を送信し、コンテンツを再生するために必要な第５の情報を受信し、自分自身を特定することができる第６の情報を、第４の情報の送信先の公開鍵で暗号化し、暗号化された第６の情報を、コンテンツに添付されている第１の情報に代わって、コンテンツに添付するようにしたので、コンテンツを再生するためのいわゆるライセンスの供給を受けるとともに、コンテンツの流通に関する情報をトレーシングするための情報をライセンスの供給者に送信することができる。

【０１９６】本発明の第３の情報処理装置および情報処理方法、並びにプログラムによれば、コンテンツを再生させるために用いられる、コンテンツに固有の第１の情報を記録し、コンテンツを保有する他の情報処理装置から、コンテンツに添付されている第２の情報、コンテンツを特定するための第３の情報、および、他の情報処理装置を特定するための第４の情報を含む第５の情報を受信し、記録されている第１の情報のうち、第３の情報によって特定されるコンテンツに対応する第１の情報を抽出し、他の情報処理装置を特定する情報を少なくとも含む第６の情報を生成し、生成された第６の情報、抽出された第１の情報を少なくとも含む第７の情報を生成し、生成された第７の情報を、第４の情報により特定される他の情報処理装置へ送信するようにしたので、ユーザにコンテンツを再生するための、いわゆるライセンスを供給するコンテンツ配信サービス事業者は、コンテンツの流通経路、コンテンツの満足度、プレビューの効果、ユーザの嗜好、あるいはユーザ個々のコンテンツ配信能力などについて分析するためのトレーシンク情報を得ることが可能となる。

【０１９７】本発明の情報処理システムによれば、第１の情報処理装置が、コンテンツを取得し、コンテンツに添付されている第１の情報、コンテンツを特定するための第２の情報、および自分自身を特定することができる第３の情報を含む第４の情報を生成し、生成された第４の情報を第２の情報処理装置へ送信し、第２の情報処理

装置から送信されたコンテンツを再生するために必要な第５の情報を受信し、第５の情報に添付されている第６の情報を抽出し、抽出された第６の情報を、コンテンツに添付されている第１の情報に代わって、コンテンツに添付するようにし、第２の情報処理装置が、コンテンツを再生させるために用いられる、コンテンツに固有の第７の情報を記録し、第１の情報処理装置から、第１の情報、第２の情報、および、第３の情報を含む第４の情報を受信し、記録されている第７の情報のうち、第２の情報によって特定されるコンテンツに対応する第７の情報を抽出し、第１の情報処理装置を特定する情報を少なくとも含む第６の情報を生成し、生成された第６の情報、および抽出された第７の情報を少なくとも含む第５の情報を生成し、生成された第５の情報を第３の情報により特定される第１の情報処理装置へ送信するようにしたので、ユーザは、コンテンツを再生するためのいわゆるライセンスの供給を受けるとともに、コンテンツの流通に関する情報をトレーシングするための情報をライセンスの供給者に送信することができ、ライセンスを供給するコンテンツ配信サービス事業者は、コンテンツの流通経路、コンテンツの満足度、プレビューの効果、ユーザの嗜好、あるいはユーザ個々のコンテンツ配信能力などについて分析するためのトレーシンク情報を得ることが可能となる。

【図面の簡単な説明】

【図１】本発明を適応したコンテンツ配信サービスを提供するために利用されるネットワーク構成図である。

【図２】コンテンツデータベースに登録されているコンテンツ管理テーブルについて説明するための図である。

【図３】パーソナルコンピュータの構成について説明するためのブロック図である。

【図４】ライセンスサーバの機能を説明するための機能ブロック図である。

【図５】ユーザ登録処理について説明するためのフローチャートである。

【図６】ユーザ登録管理テーブルについて説明するための図である。

【図７】登録ユーザが保有するパーソナルコンピュータの機能について説明するための機能ブロック図である。

【図８】パーソナルコンピュータの処理について説明するためのフローチャートである。

【図９】パーソナルコンピュータの処理について説明するためのフローチャートである。

【図１０】ライセンスおよびコンテンツ、署名および暗号、並びにユーザ情報の流れについて説明するための図である。

【図１１】コンテンツ管理テーブルについて説明するための図である。

【図１２】ライセンスおよびコンテンツ、署名および暗号、並びにユーザ情報の流れについて説明するための図

41

である。

【図１３】ライセンスおよびコンテンツ、署名および暗号、並びにユーザ情報の流れについて説明するための図である。

【図１４】ライセンスおよびコンテンツ、署名および暗号、並びにユーザ情報の流れについて説明するための図である。

【図１５】ライセンスサーバの処理について説明するためのフローチャートである。

【図１６】ライセンスサーバの処理について説明するためのフローチャートである。

【図１７】トレーシング情報テーブルについて説明するための図である。

【図１８】ライセンステーブルについて説明するための図である。

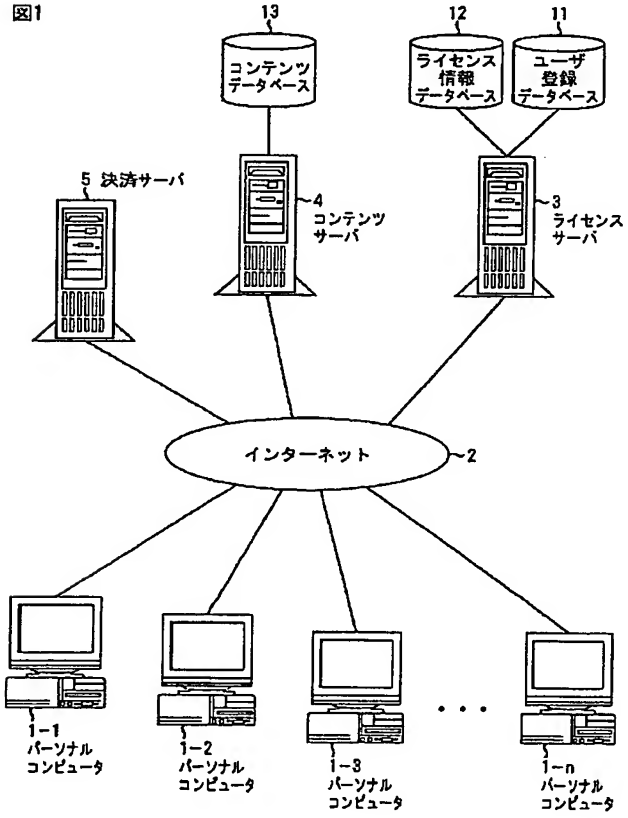
【図１９】ライセンス発行テーブルについて説明するための図である。

42

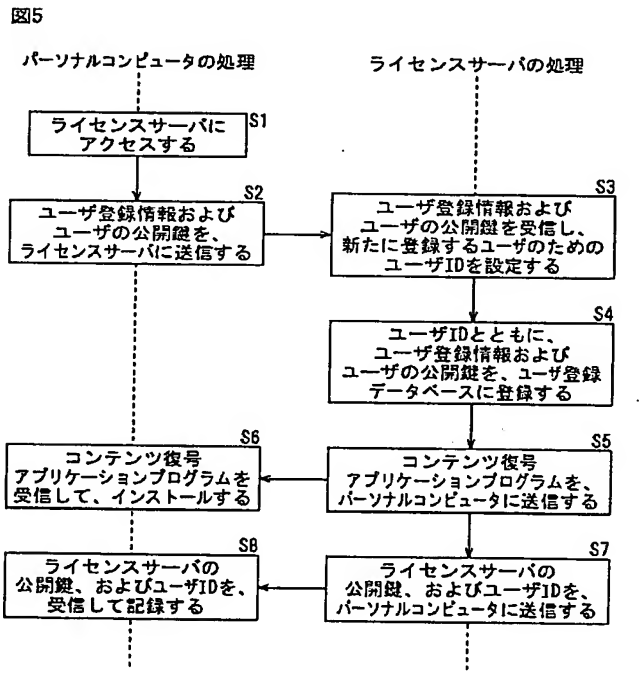
【符号の説明】

１　パーソナルコンピュータ，　２　インターネット，　３ライセンスサーバ，　４　コンテンツサーバ，　５　決済サーバ，　１１　ユーザ登録データベース，　１２　ライセンス情報データベース，　１３　コンテンツデータベース，２１　ＣＰＵ，　２４　入力部，　２７　出力部，　２６　ＲＡＭ，　３０ネットワークインターフェース，　４１　制御部，　４２　入出力インターフェース，　４３　メモリ，　４４　暗号化および復号処理部，　４５　トレーシングデータ解析部，　５１　秘密鍵記録部，　６１　制御部，　６２　入出力インターフェース，　６３　メモリ，　６４　暗号化および復号処理部，　６５　再生処理部，　７１　秘密鍵記録部，　７２　表示部，　７３　スピーカ

【図１】



【図５】



【図２】

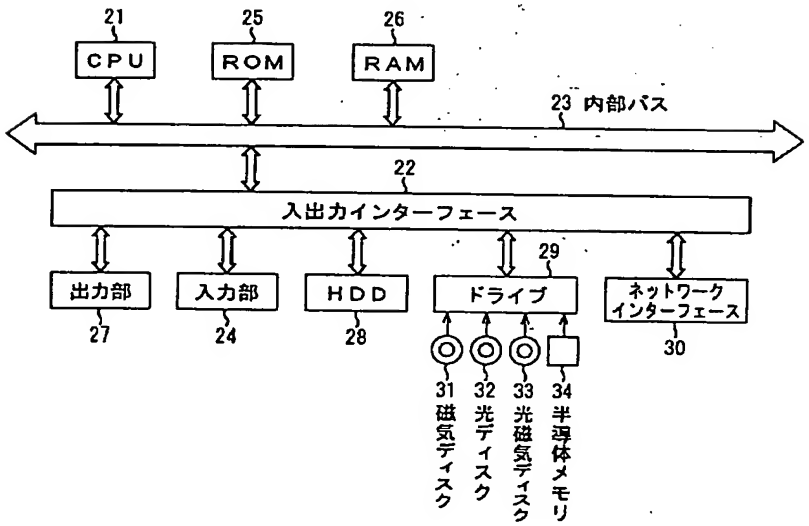
図2

コンテンツID	アドレス情報	ライセンスID	
		通常	プレビュー
000001	××××××	△△△△	○○○○
000002	××××××	△△△△	○○○○
000003	××××××	△△△△	○○○○
000004	××××××	△△△△	○○○○
000005	××××××	△△△△	○○○○
000006	××××××	△△△△	○○○○
000007	××××××	△△△△	○○○○
000008	××××××	△△△△	○○○○
⋮	⋮	⋮	⋮

コンテンツ管理テーブル

【図３】

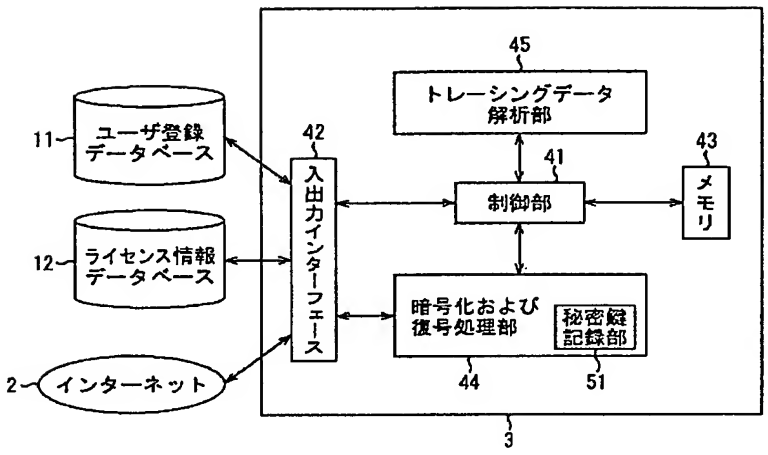
図3



パーソナルコンピュータ 1

【図４】

図4



【図６】

図6

ユーザID	ユーザ公開鍵	アドレス	ユーザ情報
a0298374	○○○○	××@△△△	·····
a0382539	○○○○	××@△△△	·····
c7984365	○○○○	××@△△△	·····
b4398878	○○○○	××@△△△	·····
a1247001	○○○○	××@△△△	·····
c8956948	○○○○	××@△△△	·····
b8758077	○○○○	××@△△△	·····
⋮	⋮	⋮	⋮

ユーザ登録管理テーブル

【図１１】

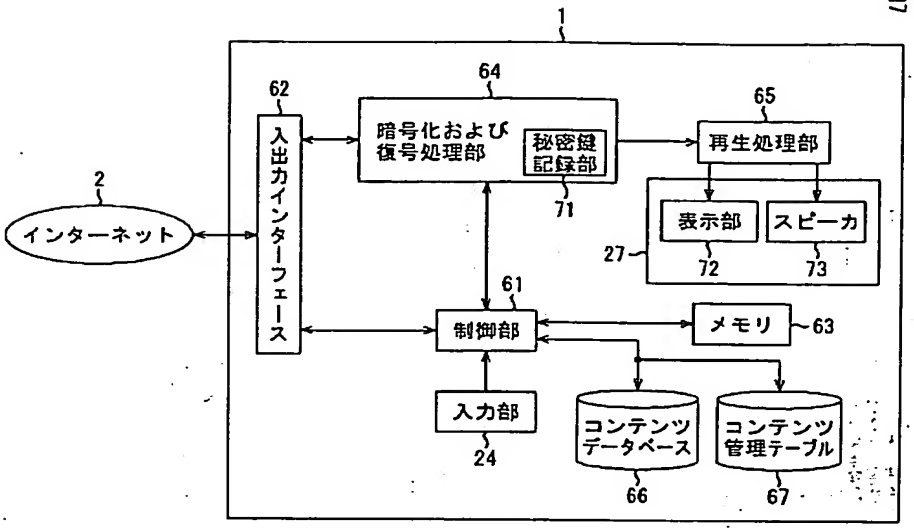
図11

コンテンツID	アドレス情報	ライセンスID	
		通常	プレビュー
000352	××××××	△△△△	○○○○
001473	××××××		
000098	××××××		○○○○
000666	××××××		○○○○
000005	××××××	△△△△	
000543	××××××	△△△△	○○○○
⋮	⋮	⋮	⋮

コンテンツ管理テーブル

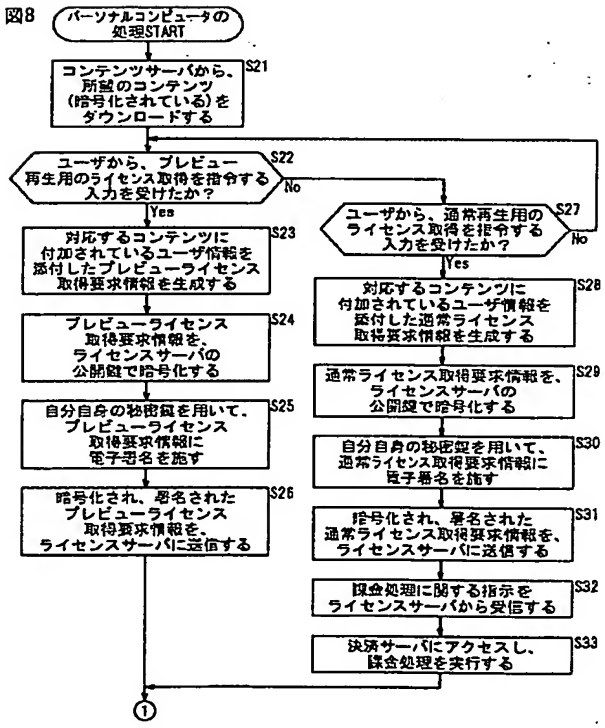
【図７】

図7



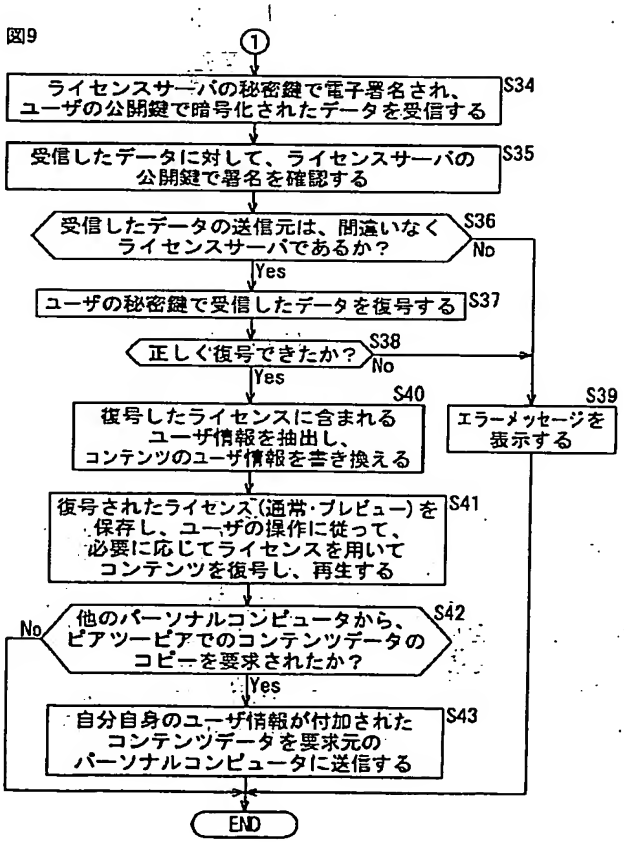
【図８】

図8

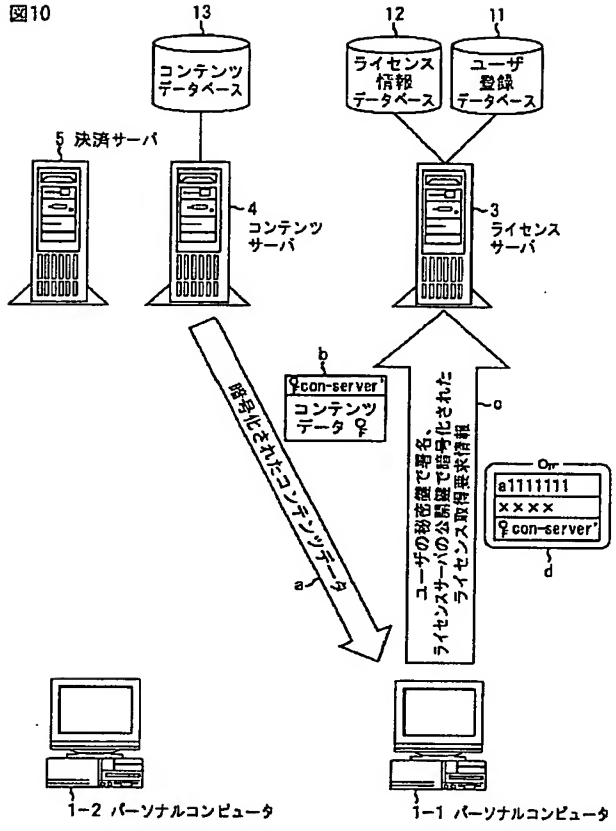


【図９】

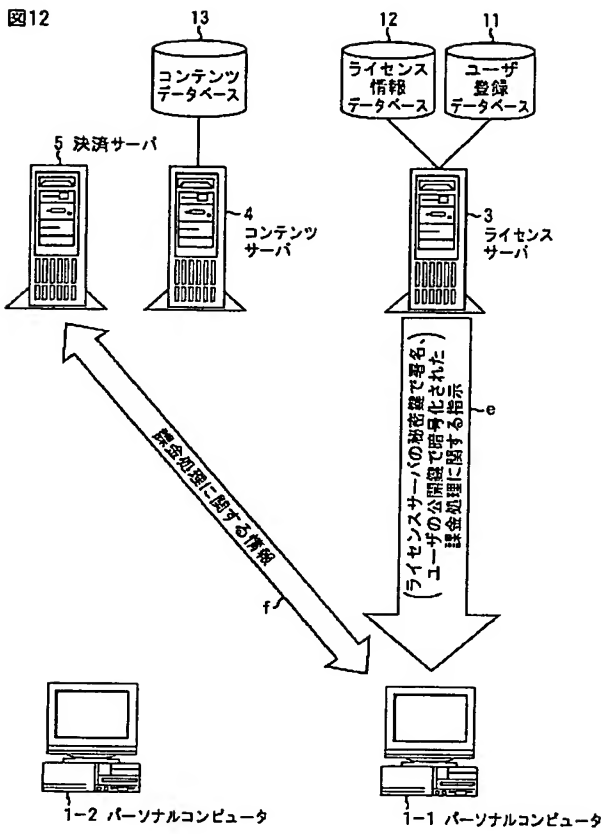
図9



【図１０】



【図１２】



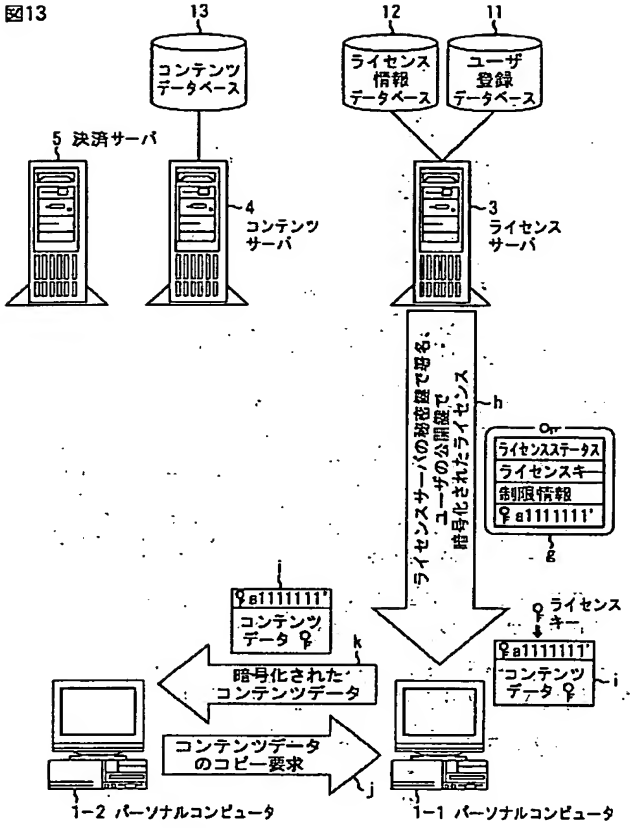
【図１７】

図17

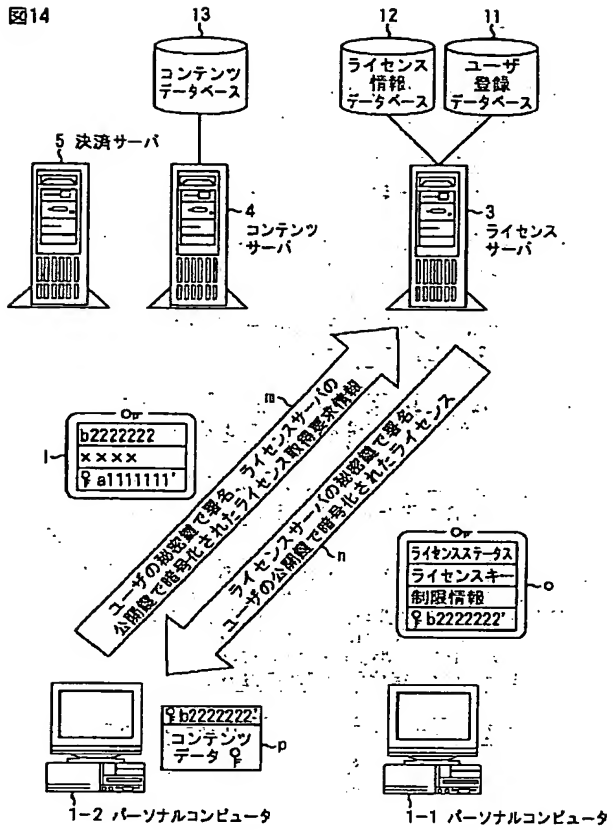
コンテンツID	ライセンスステータス	配信元ユーザID	配信先ユーザID
000005	プレビュー	con-server	a1247001
000543	プレビュー	con-server	b4398878
000098	プレビュー	a1247001	c7984365
000666	通常	c8956948	b4398878
000005	プレビュー	a1247001	a1247001
000543	通常	con-server	c8956948
000666	通常	b8758077	a0298374
000352	プレビュー	a1247001	c7984365
001473	通常	a1247001	c7984365
⋮	⋮	⋮	⋮

トレーシング情報テーブル

【図１３】



【図１４】



【図１８】

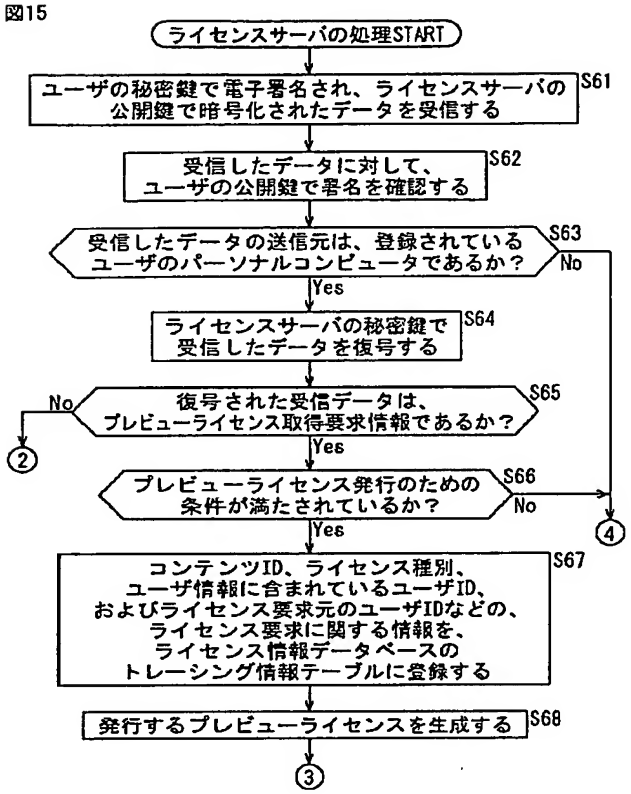
図18

コンテンツID	ライセンスID	
	通常	プレビュー
000001	△△△△	○○○○
000002	△△△△	○○○○
000003	△△△△	○○○○
000004	△△△△	○○○○
000005	△△△△	○○○○
000006	△△△△	○○○○
000007	△△△△	○○○○
000008	△△△△	○○○○
⋮	⋮	⋮

ライセンステーブル

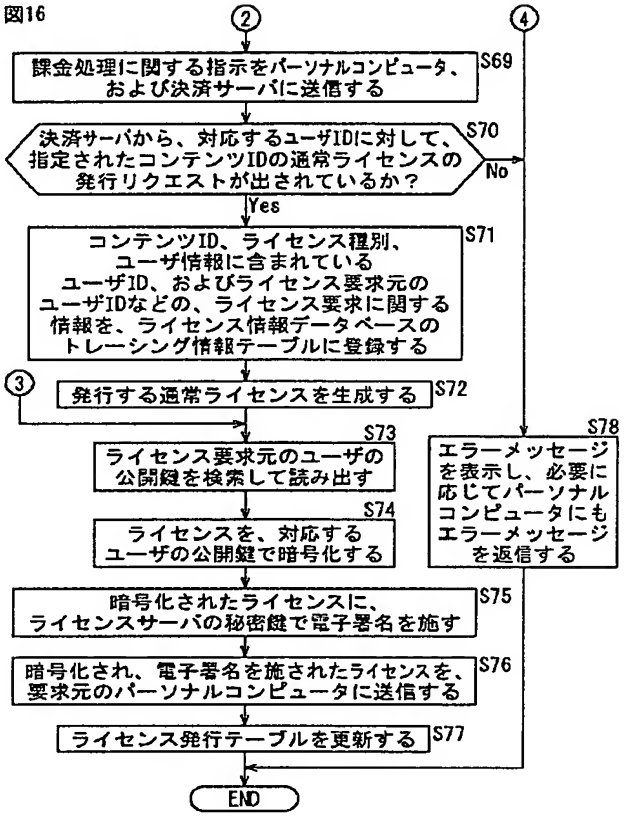
【図１５】

図15



【図１６】

図16



【図１９】

図19

ユーザID	コンテンツID	ライセンスステータス
c0037472	000098	通常
a0382539	000666	通常
c7984365	000005	プレビュー
b0117837	000543	通常
a1247001	000666	プレビュー
c8956948	000670	プレビュー
b0003422	000666	プレビュー
a0111192	000005	通常
：	：	：

ライセンス発行テーブル

フロントページの続き

(51) Int. Cl.⁷	識別記号	F I		ﾃｰﾏｺｰﾄﾞ (参考)
Ｈ０４Ｌ　9/32		Ｈ０４Ｎ	7/173	６４０Ａ
Ｈ０４Ｎ　7/167		Ｈ０４Ｌ	9/00	６７５Ｂ

7/173　　６４０　　H０４N　7/167　　Z